

- Equipment failure or human failure? (ark, Julian Gomez)
- Re: Steve Jackson Games (Jim Harkins)

- Routing tables for private switches (Simson L. Garfinkel)
- Risks of Caller Identification (David Lesher)
- More sendmail woes (PGN)
- Issue 05 (6 June 1990)
 - New computerized scoring system fails during Indy 500 (Jaime Villacorte)
 - Nuclear hair-trigger still set (Johnson v. Chain) (Clifford Johnson)
 - Network follies (Tim Shimeall)
 - Re: The A320's attacks of nerves (Danny Cohen)
 - Re: Article on A320 in Aeronautique, April 1990 (Pete Mellor, Atkielski)
 - "Computer to track down drivers without insurance" (SeanF)
 - <u>Another egregious database (Mark Anacker)</u>
 - Risks of Caller Identification (David desJardins)
 - Re: Denial of service due to switch misconfiguration (Larry Kilgallen)
 - Private mail on BBSes... (David Gursky)
 - Re: 2600 article (Henry Spencer)
- Issue 06 (7 June 1990)
 - Bei Mir ist es nicht schoen (PGN)
 - Re: Network follies (Carl Howe)
 - Bitnet FTP-ing of back issues (Paolo Mattiangeli)
 - Risk is in the eye of the beholder? (Dick Wexelblat)
 - Re: The A320's attacks of nerves (Robert Dorsett, Steven Philipson)
 - Re: Article on A320 (Karl Swartz)
 - A320 The Attacks Continue (Pete Mellor)
 - Re: Private mail on BBSes...(and the A320?) (Pete Mellor)
- Issue 07 (8 June 1990)
 - Europarliamentory software protection deadlock? (Herman J. Woltring)
 - Computer Aids May Hurt in Decision Making (Brad Dolan)
 - Re: Another egregious database (Steven Philipson, Pete Mellor, Edwin Wiles)
 - Re: Risks of Caller Identification (Jeff Johnson)
 - Re: Steven Jackson Games (Jerry Leichter)
 - Glass cockpits (A320, etc.) (Steven Philipson)
 - Stonewalling with computers (Simon Turner)
- Issue 08 (12 June 1990)
 - Liz Taylor and ``secret codes'' (PGN)
 - EEC `IT Security Evaluation Criteria' (Klaus Brunnstein)
 - Re: A 320 article in Aeronautique (Francois Felix Ingrand)
 - 2600 magazine article (Arthur L. Rubin)
 - Self-Replicating Bugs in Floppies (Warren M. McLaughlin)
 - Caller ID neither necessary nor sufficient to prevent crank calls (ark)
 - Whom Caller ID benefits and whom it does not (Peter da Silva)
 - Re: egregious database and `voluntary' data submission (Bill Janssen)
 - Egregious Database Already Exists (William M. Bumgarner)
 - Re: Another egregious database (L.P. Levine)
- Issue 09 (15 June 1990)
 - Slovenly Russian Air Defense (again) (Robert Nagler)
 - UK Hacker Goes To Jail (Anthony Appleyard ... via Robert E. Van Cleef)

Programmable parking meters (Kee Hinckley)

- Re: New computerized scoring system fails during Indy 500 (Dave Horsfall)
- Re: Caller ID for dealing with anonymous callers (Marc Shannon)
- Re: Liz Taylor and ``secret codes'' (Randal Schwartz)
- EEC ITSEC adresses (Klaus Brunnstein)
- I APOLOGIZE (Danny Cohen)
- Issue 10 (19 June 1990)
 - Risks of using commercial on-line fulltext databases (Peter D. Junger)
 - canopus.stanford.edu goes nova (Joe Dellinger)
 - Re: UK Hacker Goes To Jail (Pete Mellor)
 - Air India votes no confidence in A320 (Andrew Klossner)
 - <u>A320 near-disaster (Gregory Travis via Robert Dorsett)</u>
 - RISKS of computers in medical offices (Arthur L. Rubin)
 - More Space Telescope Problems (Karl Lehenbauer)
 - Invisibly long lines (Wilson H. Bent, Jr.)
 - Water problems (Gene Spafford)
- Issue 11 (25 June 1990)
 - The Risks of Reading RISKS (Keith Dancey, PGN)
 - "Artificial Life" out of control (Nathaniel Borenstein)
 - Update on Alcor/email case (H. K. Henson)
 - "Unbreakable Math Code Finally Broken" (J. A. Brownlee via jbr)
 - <u>A (rather old) risk of new technology (Clive Feather)</u>
 - Risk submitting papers by e-mail! (Jonathan Bowen)
 - Re: The Hubble Telescope (Tony Ozrelic)
 - Re: DEC RA90 disk failures: correction/update (David Keppel)
- Issue 12 (27 June 1990)
 - 747-400 computer problems cause excess departure delays (Jon Jacky)
 - Two 747-400 computers fail during landing approach; recall denied (Jon Jacky)
 - Re: The A320's attacks of nerves (Robert L. Smith)
 - Riskier Risks of Reading Risks (Michael Barnett)
 - Re: "Unbreakable Math Code Finally Broken" (Y. Radai)
 - Risks involved in DEC RA90 firmware upgrade procedure (Geoffrey Brunkhorst)
 - Info on carpal tunnel syndrome (Andrea Frankel via Jim Meyering and Werner Uhrig)
- Issue 13 (28 June 1990)
 - The F9 factoring result (Ron Rivest via J.Bidzos/S.Kent/S.Crocker/TMPLee)
 - <u>Risks from using laptops with cellular phones (Jan I Wolitzky)</u>
 - Re: carpal tunnel syndrome (Mike Tanner, Henry Spencer)
 - <u>Re: The Hubble Telescope (Steve Bellovin, Henry Spencer)</u>
 - <u>My A320 "Article" (Gregory Travis)</u>
 - Re: The A320's attacks of nerves (Gimli) (Robert Dorsett, J.G. Mainwaring)
 - Virus experiences in GDR (Klaus Brunnstein)
 - A misdirected letter or Chain mail (Greeny)
- Issue 14 (29 June 1990)
 - RISKS WILL BE ON VACATION (RISKS Forum)
 - Hubble (Dimitri Mihalas via Mark Bartelt)
 - Re: "Unbreakable Math Code Finally Broken" (Richard A. Schumacher)

More on the Risks of searching the Lexis fulltext database (Peter D. Junger)

- <u>Re: info on carpal tunnel syndrome (Terry Kane)</u>
- Issue 15 (26 July 1990)
 - Benefits and Risks of Knowledge-Based Systems (Brian Randell)
 - CB "Traffic Advisory Channel" petition (Mark Draughn via Peter Jones)
 - <u>New Bank Software => Problems (Jeff Johnson)</u>
 - Viper and its Formal Verification (Brian Randell)
 - Cellphone risk to ABS? (Martyn Thomas)
 - <u>Car phones and electronic systems (Tim Duncan)</u>
 - <u>Washington State Ferries slide into home (Joe Dellinger)</u>
 - Pentagon Pizza (Jim Harkins)
 - Logica Code Slows Trident (Mark Smith)
 - GAO slams FAA computer systems (Rodney Hoffman)
 - BMW Drive-by-wire (Rodney Hoffman)
 - British air defense computer suffers a "nervous breakdown" (Walt Thode)
 - British Rail signalling software problem (Pete Mellor)
 - <u>Call for Papers on Testing, Analysis and Verification (Nancy Leveson)</u>
- Issue 16 (31 July 1990)
 - Etalfried Wedd's Loan Authorization (John W. McInroy)
 - Pilots vs. automation (Henry Spencer)
 - Widespread use of computer simulations as evidence in court (Jon Jacky)
 - <u>Oklahoma computer system foulup (Steve Bellovin)</u>
 - Big Brother getting bigger (Clifford Johnson)
 - RISKS of Publicly-conducted Benchmark Demonstrations (Richard Busch)
 - Citibank, ATM, electronic transactions (Melik Isbara)
 - USAF ecm systems: software 2 years late (Martyn Thomas)
 - <u>A320 FADEC Software Diversity?? (Pete Mellor)</u>
 - Hubble problems (Eugene N. Miya)
 - Re: Pentagon Pizza (Henry Spencer)
 - More on carpal tunnel syndrome/RSI (Blake Sobiloff)
 - CTS info requested (Alan Wexelblat)
 - Risk Management in the public sector (Request for info) (Mark A. Yedinak)
- Issue 17 (2 August 1990)
 - A Tough Roach to Ho-Ho Your PC; more on bugs in sendmail (PGN)
 - BMW's 'autopilot' (Chaz Heritage via Richard Busch)
 - SIGSOFT '91, conference on critical systems preliminary announcement (PGN)
 - European Symposium on Research in Computer Security, program (Yves Deswarte)
 - Pilots vs. automation (Bob Sutterfield)
 - <u>Altitude violations and TCAS (Andrew Koenig)</u>
 - Risks of Research vs Errors (Hubble) (Dave Davis)
 - Re: Hubble Trouble (Brinton Cooper, Bryce Nesbitt)
 - RISKS of slanting computer related excerpts (pigeons) (Jay Schmidgall)
- Issue 18 (9 August 1990)
 - Roller Coasters scarier but safer than ever (Bob Felderman)
 - Risks of de facto standards (Michael L. Littman)
 - Re: 90% of research experiments fail, Risks of Statistics (Jeremy Grodberg)
 - Re: British Rail signalling software problem (Clive Feather)
 - <u>Re: A Tough Roach ... (David Collier-Brown)</u>

Issue 19 (10 August 1990)

- <u>Computers as counterfeiters? (Will Martin)</u>
- <u>Computer voice recognition monitor for gang members (Rodney Hoffman)</u>
- U.S.-supplied Saudi air defense software not working (Jon Jacky)
- Hubble Trouble: `Astonishing' error of about 1 mm (Lauren Weinstein)
- Re: British Rail signalling software problem (Pete Mellor)
- <u>Re: "compress" and the Unisys patent (Anonymous)</u>
- Re: Design for the real world (Robert Biddle)
- <u>Computer Security Applications Conference (Marshall D. Abrams)</u>

Issue 20 (14 August 1990)

- <u>NYC Parking Violations Computer called "Rogue" (Dave Davis)</u>
- Computer noise linked to stress -- computers vs. women (Allan Meers)
- <u>Response to Computers as Counterfeiters (Sanford Sherizen)</u>
- Re: 90% of research experiments fail, Risks of Statistics (Jeremy Grodberg)
- Freedom to write programs (Richard M. Stallman)
- Re: Risks of de facto standards (Bernie Cosell)
- <u>Risks of inflation (Mark Brader)</u>
- Firing (of[f]) the Fire-Control (anonymous)
- US Department Of Education -- Student Loan Nightmares (Steven Blair)
- Error blamed on human (!) (Geoff Kuenning)
- <u>Re: Computer voice recognition monitor for gang members (smv)</u>
- Virus: cautionary tale (Paul A J)
- Issue 21 (16 August 1990)
 - Space Shuttle O-Rings NOT the real problem (S. Klein)
 - RISKS of preventive maintenance (P.J. Karafiol)
 - <u>Computer-personalized scams (Allan Meers)</u>
 - Compress patent (Richard Stallman, Bill Davidsen, D.E. Sill, Henry Spencer)
 - <u>Credit "doctors" (King Ables)</u>
 - <u>Computerized monitoring of detainees (Will Martin, Paul Shields)</u>
 - Edison and workplace drugs (Gordon Letwin)
- Issue 22 (22 August 1990)
 - Re: NYC Parking Violations Computer ... "Rogue" (Christopher Jewell)
 - Debt collector proposes "total knowlege" credit database (PH)
 - More on Computerized Monitoring of "House Arrest" Detainees (Li Gong)
 - Thailand computer system (Simson L. Garfinkel)
 - A backup that worked (Steve Bellovin)
 - NCSC to be shut down (Dave Curry)
 - How to Lie with Statistics (N H. Cole)
 - Something good about Automatic Bank Tellers (Pete Mellor)
 - 13th National Computer Security Conference, October 1-4, 1990, Washington DC (Jack Holleran)
- Issue 23 (22 August 1990)
 - <u>ATMs act up; software blamed (kjd)</u>
 - Formal Verification of Safety-Critical Systems (Brian Randell)
 - Article on VDT Radiation (Jeff Johnson)
 - Terminally dumb -- substitutions (Tony Scandora)
 - Useful credit-related addresses (Simson L. Garfinkel)

Software patent issues (John Bruner)

- <u>Re: compress (David Paul Hoyt)</u>
- New Book in Computer Ethics (Perry Morrison)
- Issue 24 (23 August 1990)
 - E-mail lawsuit (Sean)
 - Re: Electronic house arrest units (D. King)
 - Proposed ban on critical computerized systems (Cameron, PGN)
 - Object Code Copyright Implications (Robert Biddle)
 - Discover Card (Brian M. Clapper)
 - Total Knowledge about all individuals (Clifford Johnson, Alan J Rosenthal)
 - <u>Re: Useful credit-related addresses (Henry Mensch)</u>
 - "Rogue Programs: Viruses, Worms, and Trojan Horses" (Gene Spafford)

Issue 25 (27 August 1990)

- Justice Department computers vulnerable (Rodney Hoffman)
- A Step Backward (Interactive Phone Service) (Theodore Lee)
- How to Lie with Statistics [once again] (Jerry Hollombe)
- Re: Something good about Automatic Bank Tellers (Jerry Hollombe, Mark Lomas)
- Re: Electronic house arrest units (Philip L Harshman, Jim Campbell, Amos Shapir, Brinton Cooper, Brian Tompsett, Mike Bell, Willis H. Ware)
- Re: Object Code Copyright Implications (Willis H. Ware, A. Harry Williams, Lars Poulsen, Gene Spafford)
- Re: Proposed ban on critical computerized systems (Pete Mellor)
- Comment on Markoff article on NCSC (Robert H Courtney via Bill Murray)
- Issue 26 (29 August 1990)
 - Stonefish the software strikes back? (Pete Mellor)
 - <u>Computers at the Campus Bookstore (Gary McClelland)</u>
 - Reverse Engineering not always a copyright issue (Joe Morris)
 - Re: Electronic house arrest units (Martin Minow)
 - Re: Proposed ban on critical computerized systems (Perry Morrison MATH)
 - Caller ID Discussion List Started (Bruce Klopfenstein)
- Issue 27 (30 August 1990)
 - Lawsuit over specification error (Martyn Thomas)
 - Hacking Illegal in UK Official! (Pete Mellor)
 - NSA Press Release on NCSC reorganization (Jack Holleran).
 - No computers on Washington State ferries (David B. Benson)
 - <u>Re: Discover Card (Will Martin)</u>
 - Re: proposed ban on critical computerized software (Al Arsenault)
- Issue 28 (31 August 1990)
 - Re: Lawsuit over specification error (Pete Mellor, Martyn Thomas, PM)
 - <u>Computer Unreliability and Social Vulnerability: synopsis (Pete Mellor)</u>
 - <u>Computer Unreliability and Social Vulnerability: critique (Pete Mellor)</u>
 - <u>Copyright Policy (Daniel B Dobkin)</u>
 - Re: Discover Card (Brian M. Clapper, Gordon Keegan)
- Issue 29 (1 September 1990)
 - What is "safety-critical"? (Nancy Leveson)
 - Re: Computer Unreliability and Social Vulnerability (David Gillespie)

- Risks of selling/buying used computers (Fernando Pereira)
- Accidental disclosure of non-published telephone number (Peter Jones)
- Issue 30 (4 September 1990)
 - Business Week on High-Tech Amusement Parks (Karl Lehenbauer)
 - Arabian heat causing problems with US weapons computers (Jon Jacky)
 - <u>Re: Stonefish mine (Chaz Heritage via Richard Busch)</u>
 - Flight simulator certification (Henry Spencer)
 - Glass cockpits (Martyn Thomas)
 - "Wild failure modes" in analog systems (Kent Paul Dolan)
 - Faultless Software (Robert L. Smith)
 - Comment on Software Reliability Synopsis (Martin Minow)
 - Database searches and counseling center confidentiality (Derek Beatty)
- Issue 31 (5 September 1990)
 - March 1989 British Rail Train Crash (Brian Randell)
 - Complexity, safety and computers (Martyn Thomas)
 - Software bugs "stay fixed"? (Martyn Thomas)
 - Re: Stonefish mine (Mark Lomas, Bill Davidsen, Bill Ricker)
 - <u>Reply to "Computer Unreliability" Stars vs Selves (Dave Davis)</u>
 - "Wild Failure Modes" in Analog Systems (Jim Hoover, Richard D. Dean, Will Martin, Pete Mellor).
- Issue 32 (6 September 1990)
 - New Roque Imperils Printers (Robert E. Van Cleef)
 - Floating Point Emulation required for Ultrix systems (Dave Wortman)
 - Re: Software bugs "stay fixed"? (Dave Parnas)
 - Re: Wild failure modes and COMPLEXITY (Rochelle Grober)
 - Re: Lawsuit over specification error (Brinton Cooper)
 - Re: Flight simulator certification (Steven Philipson)
 - Re: Lawsuit over simulator specifications (Robert Dorsett)
 - Computers and Safety (Bill Murray)
- Issue 33 (7 September 1990)
 - Critical military computer systems (Clifford Johnson)
 - Complexity, reliability, and meaningless arguments (Nancy Leveson)
 - Re: "Wild Failure Modes" in Analog Systems (Jan Wolitzky)
 - Analog vs Digital Controls (Martin Ewing)
 - <u>Chaos (Peter da Silva)</u>
 - Re: Software bugs "stay fixed"? (Bruce Hamilton, K. M. Sandberg, Andrew Koenig, Michael Tanner)
 - Boot camping (Timothy VanFosson)
- Issue 34 (8 September 1990)
 - Risks of shutdown? (PGN)
 - French prisoners use "smart cards" (Robert Nagler)
 - Instrument Software failure in BAe aircraft (Sean)
 - <u>BMW's 'autopilot' (Michael Snyder)</u>
 - Re: "wild failure modes" in analog systems (Henry Spencer)
 - <u>Re: Dealing with software complexity (Martin Minow)</u>
 - <u>Re: Software bugs "stay fixed"? (Robert L. Smith)</u>
 - Re: Computers and Safety (John (J.G.) Mainwaring)
 - Re: Object Code Copyright Implications (Dan Bernstein, Randall Davis)

Re: Accidental Disclosure of non-published phone numbers (Jeff Johnson)

Issue 35 (10 September 1990)

- Robustness of RISK architectures (Martin Minow)
- RISKS of relying on hardcopy printers (Voyager) (Tom Neff)
- Analog vs digital failure modes and conservation laws (Jerry Leichter)
- Analog vs digital reliability (Jack Goldberg)
- Re: Software bugs "stay fixed"? (Tom Neff, Stephen G. Smith, Martyn Thomas)
- Simulator classification as safety-critical (Martyn Thomas)
- Re: New Rogue Imperils Printers (Henry Spencer)
- Re: Postscript virus (Robert Trebor Woodhead)
- <u>Re: Computers and Safety (Robert Trebor Woodhead)</u>
- <u>SafetyNet '90 Conference Announcement (Cliff Jones)</u>

Issue 36 (12 September 1990)

- Railway Safe Working large analogue systems (Skillicorn)
- Re: BMW Heading Control System (A. L. Bangs)
- Re: Robustness of RISC architectures (Andy Glew, Dave Sill, Andrew Taylor, Henry Spencer, Peter Holzer, Robert Cooper, Dik T. Winter)
- Re: Computers and Safety (Peter Holzer)
- Re: Software doesn't wear out? (Bob Estell)
- Re: Software bugs "stay fixed" (Peter da Silva)
- Issue 37 (13 September 1990)
 - Expert system in the loop (Martyn Thomas)
 - Re: Railway Safe Working large analogue systems (Dave Parnas)
 - <u>Re: Analog vs digital reliability (Rob Sartin, David Murphy)</u>
 - The need for software certification (John H. Whitehouse)
 - ZIP code correcting software (Richard W. Meyer)
 - Software Bugs "stay fixed"? (Jeff Jacobs)
- Issue 38 (14 September 1990)
 - The Weakest Link (Amos Shapir)
 - <u>Relatively Risky Cars (Martin Burgess)</u>
 - <u>Re: The need for software certification (Theodore Ts'o)</u>
 - Re: Expert System in the loop (Steven Philipson, Brinton Cooper)
 - Re: Computer Unreliability and Social Vulnerability: critique (Dan Schlitt)
 - Large analog systems and NSW railroads (David Benson).
 - Analog vs Digital reliability (Bill Plummer)
 - Re: ZIP code correcting software (Bernard M. Gunther, Dave Katz)
- Issue 39 (18 September 1990)
 - Poetic Justice in a Machine Crash (Andy Glew via Paul Eggert)
 - Re: Expert system in the loop (Clifford Johnson, Peter G. Rose, Jeff Johnson)
 - I'm 99% Sure You're A Crook!!! (mmm)
 - <u>A Nightmare: Security compromise with SUN's C2 package (Caveh Jalali)</u>
 - Another risk of phone systems [anonymous]
 - <u>Desktop Publishing Fraud (Sanford Sherizen)</u>
 - Data cowboys and database abuse applicant screening (Rodney Hoffman)
 - Inside risks of INSIDE RISKS (PGN)
- Issue 40 (18 September 1990)

- Software Unreliability and Social Vulnerability (Perry Morrison)
- DTI/SERC Safety Critical Systems Research Programme (Brian Randell)
- Canadian Transportation Accident Investigation (Brian Fultz)
- <u>Risk of Collision (Brian Fultz)</u>
- Knight reference: `Shapes of bugs' (Pete Mellor)
- Issue 41 (18 September 1990)
 - Software Certification (Michael J. Konopik, Joe Marshall, Jerry Glomph Black, Martyn Thomas, Phil Windley, GaryFostel, Theodore Ts'o)

Issue 42 (22 September 1990)

- <u>Arbitration Myths (Peter Denning)</u>
- Re: Security compromise with SUN's C2 package (Li Gong)
- Re: Expert system in the loop (Henry Spencer [2], Steven Philipson [2], Walt Thode)
- Railway Safe Working large analogue systems (Peter Jones)
- Re: I'm 99% Sure You're A Crook!!! (Jerry Hollombe)
- Book suggestion: Apollo, The Race to the Moon (Martin Minow)
- Re: Knight reference: 'Shapes of bugs' (Nancy Leveson)
- ACM Conference on Critical Issues in Computing (Harold S. Stone)

Issue 43 (22 September 1990)

- Certification (Richard Platek, Paul Tomblin, John H. Whitehouse, Alan R Kaminsky, Russell C. Sorber, John H. Whitehouse, Frank Houston, BC Tompsett)
- Applicability of software curricula (Jeffrey Mogul)
- Occupational Licensing (Book Review) (Tony Harminc)
- Issue 44 (24 September 1990)
 - Arbitration Myths (Leslie Lamport, Mark S. Day)
 - Overbilled by 6 orders of magnitude (Jeff Johnson)
 - <u>Risks of "automated guided vehicles" (Brad Dolan)</u>
 - Field commanders using UNIX? (Tom Beattie)
 - Expert system in the loop (Matt Jaffe, Clifford Johnson, bahn_pr)
 - Apollo, The Race to the Moon (R.I. Cook)
 - Failed mail ("after 246 days"!) and comment on long header lines (PGN)
- Issue 45 (26 September 1990)
 - Computergate in New Jersey? (Steve Bellovin)
 - Whitehall rebuked for 121 million pound Retail Price Index blunder (Dorothy Graham)
 - Hi-tech advertising (Dave Turner)
 - Students taking exams by remote hookups (PGN)
 - Sun C2 system (Stephanie Zakrzewski)
 - Arbiters (Brian Randell)
 - <u>Re: Expert system in the loop (Amos Shapir, Jim Horning, R Horn)</u>
 - <u>Reliability of the Space Shuttle (Peter da Silva)</u>
 - Illinois Bill (Mark Brader)

Issue 46 (28 September 1990)

- Sellers Use Computer Glitch to Buy Illegal Winning Lottery Tickets (Nathaniel Borenstein)
- <u>Safer to Fly or Drive? (David Levine)</u>
- Re: Expert system in the loop (Matt Jaffe (2))

- Bookkeeping error begs for machine help -- maybe (Jim Purtilo)
- <u>Re: Hi-tech advertising (Brinton Cooper)</u>
- Re: Reliability of the Space Shuttle (Chris Jones, Henry Spencer)
- <u>Automated vehicle guidance systems (Will Martin)</u>
- Computer 'error' in the British RPI (Chaz Heritage via Richard Busch)
- Issue 47 (4 October 1990)
 - California DMV and their new computer (Cecil Lee (2))
 - <u>Report of Nat Semi clock chip flaw (Martyn Thomas)</u>
 - BA 747-400 Engine Failure (Martyn Thomas)
 - Novel on corporate computer espionage (Philip Brewer)
 - <u>CERT Advisory NeXT systems (Edward DeHart)</u>
 - Fair Information Principles (Jeff Johnson)
 - Television rating (nee universal listening) device (Tim Wood)
 - From under a Rock??? (Subliminal message lawsuits) (Ed Hall)
 - Operation Sun Devil invades the InterNet? (Ed Luke via Michael Packer via John M. Chapin)
- Issue 48 (9 October 1990)
 - Global warming or bad hardware? (Bob Campbell)
 - Equinox on A320 (Pete Mellor)
 - Ada and multitasking (Erling Kristiansen)
 - Re: Arbitration Myths (Bernie Cosell)
 - California DMV and Italian publicity (Jon)
 - <u>Government routinely ignores Privacy Act (Clifford Johnson)</u>
 - Computer sound editors are appropriate technology, not deceipt (David A. Honig)
 - Operation Sun Devil invades the InterNet? (Jonathan I. Kamens)
 - Loving Little Egypt phone freaks (Dick Karpinski)
 - CERT Advisory Update NeXT Systems (Ed DeHart)

Issue 49 (11 October 1990)

- Programmer error kills phones for 30 minutes (John R. Dudeck)
- Answering Machine Cheats at Phone Tag (Ed McGuire)
- Discovery misprogrammed (Fernando Pereira)
- Airliner story (Rich Epstein via Gene Spafford)
- An IBM interface glitch & RISKS masthead FTP instructions (Lorenzo Strigini)
- Automobile Computer RISKS A Real Life Experience (Marc Lewert)
- Re: BA 747-400 Engine Failure (Jerry Hollombe)
- Re: Equinox on A320 (Ken Tindell, Henry Spencer)
- Re: Ada and multitasking (Stephen Tihor, Henry Spencer)

Issue 50 (15 October 1990)

- Hackers blackmail UK five banks (Pete Mellor)
- Equinox on A320 (Robert Dorsett)
- Re: A320s and Northwest Airlines (Chris Davis)
- Re: Ada MultiTasking (Chet Laughlin)
- Re: Expert system in the loop (Randall Davis)
- Announcement of CPSR annual meeting (Lesley Kalmin)
- Issue 51 (16 October 1990)
 - A Schaching Development in Kasparov-Karpov (anonymous)
 - Software problem contributes to woman's death (Mike Overstreet)

Airliner story (Christopher C. Stacy, Richard Neitzel)

- Re: A320s and Northwest Airlines (Craig A. Finseth)
- Technophilia-induced problem at Educom? (R. Aminzade)
- Issue 52 (17 October 1990)
 - Re: "Pilot error" and Human Factors (P.F. Spelt)
 - Be careful of what you give away! (M. Freeman)
 - Re: Technophilia-induced problem at Educom? (Benjamin Ellsworth)
 - Passwords and chess (Steve Bellovin)
 - "Expert Systems in the Loop" explained (Martyn Thomas)
- Issue 53 (17 October 1990)
 - Lies, damn lies, and statistics... computer cabin-safety (Robert Dorsett)
 - Ada MultiTasking (Edward V. Berard, Bertrand Meyer, Robert Firth, Ray Diederich, Brian Hanafee)
 - Re: Technophilia-induced problem at Educom? (Miles R. Fidelman)
- Issue 54 (18 October 1990)
 - Flawed computer chip sold for years (Al Stangenberger)
 - The slippery slope of personal identification and tracking (Jerry Leichter)
 - <u>Technology Meets Dog; Dog Wins (Sanford Sherizen)</u>
 - Pilot error and human factors (ark)
- Issue 55 (23 October 1990)
 - Malfunction on Gambling Machine delivers \$300,000 Jackpot (John Colville)
 - Risks of Modernization (Chuck Weinstock)
 - Airliner story (Ellen Cherniavsky)
 - Summary of A320 report on W5 (Wayne Hayes)
 - Boeing 777 to use fly by wire (Robert R. Henry)
 - Re: Technology Meets Dog; Dog Wins (Dan Sandin)
 - Stick-up At Banks (Paul Johnson)
 - Re: Kasparov's sealed move (Peter Rice)
 - Computerized cars and ham radio interference (Rich Wales)
 - Programmer error, not language flaw (Stuart Friedberg)
- Issue 56 (29 October 1990)
 - Disabling software by remote control leads to law suit (Jerry Leichter)
 - Cellular phone snooping (Alan Wexelblat)
 - <u>Access to gov't computer files (John Sullivan)</u>
 - DTP and fraud (Robert Slade)
 - Funny Bible update (Paul M Dubuc via Fred Gilham)
 - Re: "Risks of modernization" -- train/pipeline accident
 - ... (Martin Minow, Bill Davidsen, Roy Smith, Peter Amstein)
- Issue 57 (4 November 1990)
 - \$6.3 million electric bill (Mark W. Schumann)
 - Drug RISKS to software ?? (Simon Rosenthal)
 - <u>More of what really goes wrong (John Rushby)</u>
 - <u>Automotive electronic engine control failure modes (Dave Davis)</u>
 - Re: Laxness, not modernization, at fault in train wreck (Chuck Weinstock)
 - Train Wreck and Weight Estimates (anonymous)
 - Re: Risks of Modernization (Gerald Stafleu)

- Re: Access to gov't computer files (Brinton Cooper)
- Call for papers -- ACM SIGSOFT '91 (Nancy Leveson)

Issue 58 (4 November 1990)

- Canadian Auditor-General fears computer sabotage (David Sherman)
- U.S. Sprint new calling card system (Jim Morton)
- <u>Chilling Advertisement (Cindy Tittle)</u>
- Prodigy Censors Users (Dave King)
- "Expert Systems in the Loop" explained (Randall Davis)
- Re: Airliner story (Christopher C. Stacy)

Issue 59 (9 November 1990)

- "Software fault hits payphones" (Martyn Thomas)
- Plain paper faxes keep copy of received material (Jan Christiaan van Winkel)
- Customers limiting programmer access to their systems (Jim Kimble)
- Student hackers arrested (Dave King)
- Sprint's new calling card (anonymous)
- Employer's use of credit reports (Jerry Leichter)
- <u>Computers lead to greater monopolization? (Jim Griffith)</u>
- Risks when computers replace humans (Martyn Thomas)
- Villanova University Computer Ethics course Group Project (J. Gacad et al.)
- "The Devouring Fungus" at a bookstore near you (Gene Spafford)
- 4th Annual Computer Virus & Security Conference (Gene Spafford)

Issue 60 (14 November 1990)

- Computer Mishap Forces shift in Election Coverage (bahn_pr)
- <u>Voting electronically from home (revisited) (John Roe)</u>
- Barclays' security: apologies! (Pete Mellor)
- Juicy 911 RISKS (Steve Smaha)
- Re: UK Software Engineer Certification (Brian Tompsett)
- Software Protection Tool (Dave Erstad)
- Sprint's voice-card system (Steve Elias, Jerry Glomph Black)
- Re: Carbons (Douglas W. Jones)
- Your Flood Stories, Please (Lindsay F. Marshall)
- Corrected version of Virus Conf announcement (Gene Spafford)

Issue 61 (16 November 1990)

- Police technology; mailing list hyperstacks (Lotus) (Jerry Leichter)
- Privacy concerns about Lotus "Marketplace" (Jeff E. Nelson, Rick Noah Zucker)
- Kuwaiti citizen database (Jonathan Leech)
- Gas pump inaccuracies? (Paul Schmidt)
- "It's the computer's fault" (Andrew Klossner)
- Re: Voting electronically from home (Li Gong, Frank Hage, Dan Sandin)
- Re: Computer Mishap Forces shift in Election Coverage (Tom Perrine)
- <u>Election coverage software (Gary Cattarin)</u>
- Re: Juicy 911 RISKS (Amos Shapir)
- <u>Ada Remarks (Paul Murdock)</u>
- Issue 62 (19 November 1990)
 - Playboy jammer who jammed Hefner's 'jamas gets jammed (PGN)
 - Telephone cable cut eliminates O'Hare tower communications (Richard I. Cook)

Tomatoed 911 (Rob Boudrie)

- Computer-Aided Gerrymandering (Steve Summit)
- GOES mirror problems caused by oversimplified analysis (Henry Spencer)
- Re: Privacy concerns about new Lotus "Marketplace" product (Dan Aronson)
- AFCEA's 2nd Annual Military / Government Computing Conf/Exp (Jack Holleran)
- Issue 63 (21 November 1990)
 - Lotus Marketplace cont'd (Marc Rotenberg, Eric Dittman)
 - Insurance Perfidy (Sharon Cregier)
 - [anonymous] author identifies anonymous referee (anonymous)
 - Reuters Holdings PLC and shouldering the blame? (Sameer Mithal, PGN abstracting)
 - MD-11 test flights over the pole (Henry Spencer)
 - Soc.Sec.No. on Driver's Lic. in Mass. (William Ricker)
 - Tomatoed 911 (Tim Steele)
- Issue 64 (21 November 1990)
 - <u>Re: Voting from home electronically (Alan Jeffrey, Steve Bellovin, Brad Templeton, Henry Spencer, Peter da</u> <u>Silva, P.J. Karafiol, Barbara Simons, Joseph R. Beckenbach, Alan Marcum, K.M. Sandberg, Chris Maltby, R.</u> <u>Simkin, Flint Pellett)</u>
 - Re: Election coverage software (Gregory G. Woodbury)
- Issue 65 (6 December 1990)
 - <u>A fondness for turkeys (Pete Mellor)</u>
 - Heads-up "Holograms" of Runways to assist in landings? (Richard Wood)
 - Airline safety (John Sullivan)
 - As the spacecraft turn (Steve Bellovin)
 - NeXT microphone problem? (E. Loren Buhle, Jr.)
 - Risks of global networking (Hank Nussbacher)
 - Technological Risk, by H.W. Lewis (Jake Livni)
 - Hackers Accessed NASA's Phones (anonymous)
 - Hacker view of the "Legion of Doom" sentencing in Atlanta (EmmanuelGoldstein)
- Issue 66 (7 December 1990)
 - COMPUTERS AT RISK: Safe Computing in the Information Age (Marjory Blumenthal)
 - <u>COMPUTERS UNDER ATTACK (Peter Denning)</u>
 - <u>Re: ``Hackers Accessed NASA's Phones'' (Jerry Hollombe)</u>
 - Responses to article on "Legion of Doom" sentencing (Gary Cattarin, King Ables, Brinton Cooper, Mark E. Levy)
- Issue 67 (7 December 1990)
 - Airline safety (Donald A Norman)
 - Voter identity and Dial-A-Vote (Lauren Weinstein, Glen Overby, Paul Peters, Andrew Klossner, Dan Sandin, Frank Kuiper, Adams Douglas)
 - "Little pitchers have big ears": yet another ATM RISK (zowie)
 - <u>Billing software wastes money (Phil R.M.)</u>
- Issue 68 (14 December 1990)
 - Recent RISKS Mail to CSL.SRI.COM (PGN)
 - Many Bills Are Found Incorrect on Adjustable Rate Mortgages (Saul Tannenbaum)
 - Loughborough (Rob Thirlby via Brian Randell)
 - Gender and computer anxiety (Rob Gross)

- <u>Computerized USA Phone Directory (Allan Meers)</u>
- Getting out of Lotus' "Household Marketplace" (TDN)
- <u>Re: a fondness for turkeys (Haynes)</u>
- Call for Papers 14th National Computer Security Conference (Jack Holleran)
- Issue 69 (18 December 1990)
 - "Computer Models Leave U.S. Leaders Sure of Victory" (Jon Jacky)
 - Re: Airline safety (Jim Rees)
 - The Incredible Lightness of Reference (Jerry Leichter)
 - Unexpected effects of PC's (Jerry Leichter)
 - Long-distance printing, or the risks of being well-known (Jerry Leichter)
 - <u>Covert communication through public databases (Larry Hunter)</u>
- Issue 70 (18 December 1990)
 - Telephone Voting (Bill Murray)
 - Voting Technology (William W. Plummer)
 - Re: Hacked NASA phones (Barton Christopher Massey)
 - Re: "Legion of Doom" (Irving Wolfe, Mike Black)
 - <u>Computer Virus as Military/Political Weapon? (Sanford Sherizen)</u>
 - Request for Info on Undergraduate Computer Security Classes (Al Arsenault)

Issue 71 (19 December 1990)

- Re: "Computer Models Leave U.S. Leaders Sure of Victory" (Marcus J. Ranum, Karl Lehenbauer, Bob Estell)
- <u>Compass Airlines disrupted by possible computer attack (Sarge)</u>
- Punny user interface [anonymous]
- Process control risks discussed in IEEE Software (Andy Oram)
- <u>Unexpected effects of PC's (P.J. Karafiol, ark)</u>
- Missing reference (Jerry Leichter)
- A semi-folk tale on the risks of being well-known (Daniel P Dern)
- Re: the risks of being well known (Scott Schwartz)
- Re: Organizational Aspects of Safety (Charlie Martin)
- Issue 72 (19 December 1990)
 - Re: Computer Models Leave U.S. Leaders Sure of Victory (Richard Schroeppel)
 - Re: Voting Technology ... (Brian Rice, Jerry Leichter, Michael J. Chinni, Lauren Weinstein)
 - Re: Legion of Doom (John Boyd, K. M. Sandberg, Brendan Kehoe)
 - Value of data integrity (Mahan Stephen)
- Issue 73 (21 December 1990)
 - HERO Hazard of Electromagnetic Radiation to Ordnance (Rodney Hoffman)
 - Washington (state) E-mail Privacy Suit (Peter Marshall)
 - Re: Process control risks discussed in IEEE Software (Nancy Leveson)
 - Re: "Computer Models Leave U.S. Leaders Sure of Victory" ... (P.G. Capek, Jerry Hollombe, Neil Galarneau)
 - Risks of Automated Collections and a Happy Ending (L.J. Hoffman)
 - Re: The topic that wouldn't die: telephone voting (Gregory G. Woodbury)
- Issue 74 (3 January 1991)
 - Vicious elevator door failure recovery (Curtis Jackson)
 - Dehumanization by old Cobol programs; how to get more junk mail (Darrell Long)
 - <u>Computer data putting history out of reach (Jay Elinsky)</u>
 - Re: Computer Age Causes Key U.S. Data To Be Lost Forever (Joe A. Brownlee)

- Re: computer "warfare" (John Abolins)
- Re: "Computer Models Leave U.S. Leaders Sure of Victory"... (Jeff Griffen, David Holland, John C Slimick, David Wright)
- Trojan in MS-DOS 4.01? (John Chapman Flack)
- <u>Re: Organizational Aspects of Safety (Nick Szabo)</u>
- A RISKy video store kiosk (R. Aminizade)
- Call for papers, VDM '91 (Hans Toetenel)
- Issue 75 (7 January 1991)
 - NY area fiber-optic telephone cable severed; extensive effects (PGN)
 - <u>British military information stolen (Charles Bryant)</u>
 - <u>Wargames and Reality (Robert Firth)</u>
 - Re: Vicious elevators (Tom Lane, Mark Brader, Roland G. Ouellette, Jake Livni)
 - <u>Re: Dehumanization by old Cobol programs (Karen Ward)</u>
 - Re: "Computer Models Leave U.S. Leaders Sure of Victory" (Henry Spencer)
 - Re: "Computer Age Causes Key U.S. Data To Be Lost Forever" (Rick Smith)
 - Re: "Little pitchers have big ears": ATM Risk (Michael McKay)
 - Cars and Automation [again] (Balakumar)

Issue 76 (9 January 1991)

- Suit says Nissan Fired 2 After reading e-mail (Rodney Hoffman)
- Email flash from the past (Paul Eggert)
- Re: Cars and Automation: Yes, a computer problem! (Gregory G. Woodbury)
- Another train crash in London (Olivier M.J. Crepin-Leblond)
- Re: NY area fiber-optic telephone cable severed (Tony Scandora)
- Re: Vicious elevator door failure recovery (David Magnay, Olivier M.J. Crepin-Leblond, Michael J. Chinni, Russell McFatter)
- Journal of Computer Security, Call for papers (Sushil Jajodia)

Issue 77 (11 January 1991)

- Computer program gives police a bum rap (David A Smallberg)
- Unusual distance metric could waste consumers' time and gas (David A Smallberg)
- Computers Stolen in the USSR (Sanford Sherizen)
- Re: British military information stolen (Stephen Carter)
- Vicious Subway Cars (Ed Ravin)
- <u>Vicious Doors on London Underground/Network South-East (Pete Mellor)</u>
- Defence of British Rail/Network SouthEast (David Green)
- RISKS of computer-assisted emergency dispatch systems (Ed Ravin)
- 2nd IFIP Dependable Computing Conference (Rick Schlichting)
- <u>First Conference on Computers, Freedom & Privacy (Dorothy Denning)</u>

Issue 78 (22 January 1991)

- (No) Viruses in Iraq's EXOCET? (Klaus Brunnstein)
- <u>Risks of NOT believing war game models (Bob Estell)</u>
- <u>Re: MoD computer stolen in UK (Olivier M.J. Crepin-Leblond)</u>
- Re: Computer program gives police a bum rap (William H. Glass)
- Voting by Phone (Evan Ravitz, PGN)
- (More) word processor atrocities (Pete Mellor)
- Issue 79 (23 January 1991)
 - Lotus Marketplace (various sources)

UK firms poor on computer health (Olivier M.J. Crepin-Leblond)

- Data privacy abuse in Australia (Phil Clark)
- MasterCard policy opens door to crooks (Marv Westrom)
- Issue 80 (25 January 1991)
 - 7th Chaos Computer Congress, Hamburg, 27-29 Dec 1990 (Klaus Brunnstein)
 - San Francisco taxes its computer people rather than its property owners (PGN)
 - Not risk versus convenience, but risks of conveniences (Jack Campin) [Loo-Hoo!]
 - Re: Computer program gives police a bum rap (Mark Hull-Richter)
 - Re: Lotus Marketplace (Richard A. Schumacher)
 - MasterCard policy opens door to crooks (Steve Pozgaj, anonymous)
- Issue 81 (28 January 1991)
 - Risks in forensic use of dental and medical records (Sanford Sherizen)
 - Kinking Foreign-sold Military Equipment (Karl Lehenbauer)
 - Patriot missiles (Phil Agre)
 - Electronic cash completely replacing cash (David 'Witt')
 - Re: San Francisco taxes its computer people ... (Bill Davidsen)
 - Re: Random Voting IDs and Bogus Votes (Vote by Phone) (Li Gong, Kathy Vincent)
 - Re: Lotus Marketplace (Samuel Bates)
 - Re: Superloo (Lars-Henrik Eriksson)
- Issue 82 (29 January 1991)
 - Re: Patriots: SDI, etc. (Dave Parnas, Nathaniel Borenstein, Phil R. Karn, Hans Mulder)
 - Re: Patriots and electronic cash (Karl Kluge)
 - Re: Electronic cash completely (David Lamb, Larry Nathanson, Randal L. Schwartz, K. M. Sandberg, Peter da Silva, Richard A. Keeney)
- Issue 83 (29 January 1991)
 - Risks of automatic flight (flying at low level) (Olivier M.J. Crepin-Leblond)
 - Broadcast local area networks are a'comin (Tom Lane)
 - Re: Risks in forensic use of dental and medical records (Jim Purtilo)
 - Re: Patriots (Clifford Johnson, Donald L. Wegeng)
 - Re: Random Voting IDs and Bogus Votes (Raymond Chen, Colin Plumb)
 - Call for Papers, 7th Computer Security Applications Conference (Daniel Faigin)
 - Call for papers, Theorem provers in circuit design (Victoria Stavridou)
- Issue 84 (30 January 1991)
 - It's not always pilot error" Official! (Pete Mellor)
 - IRS overbills for \$1B interest (PGN)
 - <u>Re: Patriots (Dave Parnas)</u>
 - Re: Risks of automatic flight (flying at low level) (Brinton Cooper)
 - <u>Automated brokerage service (Kent M Pitman)</u>
 - Re: Broadcast local area networks are a'comin (Brinton Cooper, P.J. Karafiol)
 - <u>Re: Electronic cash (Bob Stratton, Rick Smith, Stephen Perelgut, Art Medlar, who-news?, Ed Ravin, Leslie</u> <u>DeGroff)</u>
- Issue 85 (31 January 1991)
 - Benefits of Computers, Valentine's Day Edition (Jay Elinsky)
 - Re: Auto Pilot Problems (David B. Horvath)
 - Re: Risks of automatic flight (Gordon D. Wishon)

- Re: Patriots (Alex Bangs, Jerry Leichter, Martyn Thomas, Henry Spencer, Frank Ritter, David B. Horvath)
- Re: Broadcast local area networks are a'comin (Russ Housley, Frank Letts, Rich Rosenbaum, Ian Clements)



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

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



Peter G. Neumann <neumann@csl.sri.com> Thu, 31 May 1990 13:18:38 PDT

Welcome to VOLUME 10. RISKS will be beginning its SIXTH year on 1 August 90, although it will soon go into a first-month-of-the-summer sporadic mode until then.

For FTPers who previously complained about the unfriendly sort order produced by the directory commands, you probably noticed that we recently switched the archive issue-number file name extensions to double digits (e.g., <u>RISKS-9.01</u>,

02, 03, etc.) and the volume summaries to RISKS-i.00, for i=1 to 9. Beginning with this issue we now have double-digit volume numbers for volume 10 and beyond, but the original single-digit volume numbers remain for the first 9 volumes. Beginning with this issue, ALL issue numbers will appear as two-digit numbers, even in the headers. (No volume has exceeded or will exceed 99 issues, a decision that ensures that the volume summary issues will be not much larger than RISKS-9.98 = RISKS-9.00, which was the largest yet.)

Astoundingly, there is always someone going back to get the early issues, which affords an interesting chronological perspective of where we've been and how we got to where we are now. The historical archive also gives lots of clues as to what we need to do better in the future...

Thanks for your patience through the multiple-copy ordeal. The various manifestations of it all seem to have been rectified on my end, although I still hear reports of problems elsewhere. PGN

Word Perfect Software Upgrade Crashes Utah Phone System

<m1wmk00@fed.UUCP> Thu, 31 May 90 10:16:32 +0100

>From an Infoworld article on Word Perfect ("Leader of the Pack," pp. 45-6, May 23, 1990):

"When [Word Perfect] 5.0 shipped in May 1988, the company underestimated the demand for telephone support. Although it bought additional phone lines, traffic was so heavy that calls to the support department brought down the toll-free systems for the state of Utah, including phone systems for American Express, Delta Airlines, and the Latter Day Saints Church."

Bill Kules, Automation and Research Computing, Federal Reserve Board,Washington, DCwmk@fed.FRB.GOVPhone: (202) 452-3933

Army finds new battlefield system vulnerable to software sabotage

Jon Jacky <ON@GAFFER.RAD.WASHINGTON.EDU> Thu, 31 May 1990 21:54:24 PDT

[More details on this item, first noted in RISKS-9.90.]

Here are excerpts from a page 1 story in MILITARY AND AEROSPACE ELECTRONICS, vol 1 no 5, May 1990:

VIRUSES COULD CRASH U.S. BATTLE SYSTEM by Lisa Burgess and Tobias Naegele

WASHINGTON - Computer viruses could crash critical battlefield command and control computers, according to a draft version of the Army's new Command and Control Master Plan. The report says the Army's Maneuver Control System, touted by developer TRW Inc. as the "integrating node" of the Army's command and control battle plan, is vulnerable to sabotaged software designed to undermine and disrupt operations.

... The four-page subsection, titled "Subversive Software" and buried 10 items deep in a section on camouflage, warns that "contractor-developed non-developmental item (NDI) and `homegrown' software each present unique [software surity] problems that must be addressed."

Generated by the Army's Combined Arms Combat Developments Activity at Fort Leavenworth, Kan., the report raises three questions about the potential for software sabotage to damage the \$1.3 billion MCS battle management network:

- Could virus software implanted in the system during the design phase attack MCS at a later date?
- Could an agent introduce a virus during combat by surreptitious access to a workstation?
- Could an enemy use a captured workstation to introduce a virus over the radio network?

"Under its present configuration," the report states, "the answer is yes with regards to MCS."

... Defense contractors say any system using the sort of off-the-shelf hardware and software utilized in MCS and ATCCS --- the Army Tactical Command and Control System --- is potentially vulnerable to virus attacks. ...

- Jon Jacky, University of Washington, jon@gaffer.rad.washington.edu

Caller*ID illegal in Penn

<tim@ggumby.cs.caltech.edu> Thu, 31 May 90 10:44:27 PDT

>From the Los Angeles Times, May 31, 1990, p. D2:

Court Rules Against Caller I.D.: Bell of Pennsylvania's caller-identification service is an invasion of privacy and violates the state's wiretap law, a state court ruled. The decision reverses an order by the state Public Utility Commission allowing Bell to offer the service. The service would let people know who is calling before they pick up the phone, even if the caller's number is unlisted. Several other regional phone companies already offer the service.

[Also noted by schwartz@groucho.cs.psu.edu (Scott E. Schwartz).]

Court Declares Caller*ID Illegal

<leichter@LRW.COM> Thu, 31 May 90 11:29:18 EDT

[From the New York Times, Thursday 31-May-90, Page D1]

Services Identifying Caller Held Illegal In Pennsylvania, By Keith Bradsher

A Pennsylvania court ruled yesterday that services that identify the telephone numbers of callers represent an illegal invasion of privacy.

The verdict was the first in the nation on the legality of such services. The five judges of the Commonwealth Court, a mid-level state appellate court, ruled unanimously that caller identification services ... violate Pennsylvania's wiretap law.

All five judges found that the services violate the law even when telephone companies allow some customers to block the release of their telephone numbers. And the court ruled by a 3-2 vote that the services violate privacy protections offered by the Pennsylvania Constitution.

"In the framework of a democratic society, the privacy rights concept is much too fundamental to be compromised or abridged by permitting Caller*ID," Judge Doris A. Smith wrote in the majority opinion....

But Bell of Pennsylvania criticized the ruling. "Because of this decision, Pennsylvanians are being deined a service they eagerly want and badly need a weapon against harassing, threatening or obscene calls," [a spokesman said].

Three Options for Panel

The Commonwealth Court hears appeals of decisions by state and local administrative bodies in Pennsylvania, and its decisions may be appealed to the Pennsylvania Supreme Court. John F. Povilaitis, the chief counsel of the Pennsylvania Public Utility Commission, said his office would review yesterday's decision and make a recommendation to the commissioners within a few days.

[He] said the commission had three options: to ask [for a rehearing], to file an appeal before the Pennsylvania Supreme Court, or to allow the decision to stand.

Bell of Pennsylvania was not named as a defendent in the case. But [it] said it qualified as a party [and could appeal if the PUC chose not to].

Bell ... filed with the commission on June 18, 1989 for permission to offer caller identification. The commission approved the filing on Nov. 9 and the company scheduled service to begin Jan. 9. But a Commonwealth Court judge blocked the service pending judicial review.

The suit was filed against the P.U.C. by the state's Office of the Consumer Advocate, the [ACLU], the Pennsylvania Coalition Against Domestic Violence and the Consumer Education and Protective Association.

[Caller id is now] widely available in [five states] and on a limited basis in [three others] ... according to ... a spokesman for Bell Atlantic Corporation, the parent of Bell of Pennsylvania. Phone companies in nine other states and Washington are seeking to introduce caller identification. Long-distance companies, including [AT&T], also offer caller identification to some businesses with 800 and 900 numbers. Yesterday's decision ... did not address whether long-distance companies should stop providing information for Pennsylvania callers.

"We have to see how, if at all, this ruling affects AT&T," said ... a spokesman for the company.

Privacy Issue Cited

Bell Atlantic and other defenders of caller identification have argued that the services discourage obscene callers and protect the privacy of people receiving calls by allowing them the choice of not answering. But the court ruled explicitly that the privacy of people making calls is more important.

The court found that caller identification services function as call-tracing devices, which under the Pennsylvania wiretap statute may be used only under certain circumstances. The court noted that Pennsylvania requires the consent of all parties before a telephone conversation may be recorded.

As of December, there were 15 other states with similar requirements. The remaining states and Federal law allow taping with the consent of one party. But [FCC] rules require that all parties to an interstate or international call be aware they are being taped.

The Pennsylvania wiretap statute contains wording similar to the Federal wiretap statute. Bills are pending in the House and Senate that would amend the Electronic Communications Privacy Act of 1986 to make caller identification explicitly legal while requiring that telephone companies give customers the option of blocking release of their telephone numbers. A subcommittee of the Senate Judiciary Committee has scheduled a hearing for June 7 on caller identification.

[Because of the remarkably complex tradeoffs between defensive functionality and offensive violations of rights, this item seems worth including in its entirety for its intense educational value. PGN]

✓ Denial of service due to switch misconfiguration

<marc@ATHENA.MIT.EDU> Thu, 31 May 90 03:15:15 EDT

The Massachusetts Institute of Technology runs its own 5ESS switch to provide telephone service on campus. This has significant benefits, including many different telephone classifications (office, dormitory, etc), a modem pool, and ISDN phones in the offices which pay for them (most do).

This week, I discovered what I consider a serious problem, however. A friend was at the Massachusetts General Hospital (MGH) for surgery. (I'll save you the suspense: the surgery went well.) I wanted to call and check on him to see how the surgery went. I called the hospital's main number, and was transferred

to his room, except the phone was busy, so the operator gave me his phone number.

The next day, I attempted to call his room, only to be greeted with "I'm sorry, but your call cannot be completed as dialed...." I thought about the situation, and after placing a call to the MGH operator, discovered that my friend was in a brand new building with a brand new exchange all its own. I called the MIT operator, who told me that the number I was trying to reach was in Petersburg, over a half hour away (I can see MGH from my room). I finally convinced her that this was a number at MGH, but she told me that she couldn't connect me. My phone is only able to make local calls, so I called a friend who works in the same office as the people who run the switch. They couldn't make the call. In other words, neither the operator nor the top class of phone could make the call.

Today, I called MIT's help line, and described my problem. Within several hours, my theory was confirmed. The switch simply didn't know the new exchange existed. It turns out, that as a "client," MIT doesn't get automatic updates when new exchanges are created. Without this information, the switch has no clue how to bill the caller, or even if it should let the caller make the call. So it assumes the worst case, and disallows anyone from making the call. The switch had to be manually programmed with the necessary information about the new exchange.

This worries me, as someone who isn't as familiar with telephone switching equipment might not have known what caused it, assumed it was his/her fault, and been denied service because of it. It is surprising, to me that our switch is not configured to take updates of this kind of information automatically from the New England Telephone switches it talks to. I was trying to call a hospital; fortunately it was not an emergency. My workstation has dynamic nameservice; my doesn't my telephone switch? Marc Horowitz

✓ Equipment failure or human failure?

<henry@zoo.toronto.edu> Wed, 30 May 90 23:19:46 EDT

Some little while ago, Risks published the report of a flight crew landing an airliner in Britain after a very difficult time with wind readings of 100+ knots and repeated equipment failures (in a "glass" [computerized] cockpit). There is an interesting sidelight on this in the May 2 issue of Flight International:

CAA appeals for CHIRP pilot to step forward

The UK Civil Aviation Authority is publicly appealing to an unknown pilot to file a Mandatory Occurrence Report about a serious digital cockpit systems failure which it is unable to investigate, because the airline pilot involved reported it through a confidential reporting system. Investigators and airline maintenance staff have no access to details of the apparently first-time incident. The MOR would allow the aircraft to be identified and its cockpit systems failures identified...

[Recap of incident, as reported by pilot.]

The confidential human factors incident reporting program (CHIRP) was designed to encourage pilots who have experienced a potentially dangerous incident because of human error to report it without fear of any disciplinary repercussions.

It is unclear why this pilot used CHIRP, because there is no indication of human error -- only bad weather and systems failure...

[More recap.]

One really has to wonder just what really went on on that flight. Use of CHIRP might seem appropriate to a pilot fearful of management reaction to criticism of electronic aircraft, but as a result the people who want to investigate the problem are hamstrung, doubts are cast on the accuracy of the report, and if it *is* factual, that aircraft is still in service and potentially a lethal hazard to crews and passengers.

Henry Spencer at U of Toronto Zoology

uunet!attcan!utzoo!henry

More on the Steve Jackson Games raid

<man@cs.brown.edu> Thu, 31 May 90 17:03:04 EDT

I have a friend who's involved with Steve Jackson games and here is his response to the articles that have appeared recently in RISKS. -Mark [I had to edit a bit to make it self contained,

rather than including all of the previous items. PGN]

Date: Thu, 31 May 90 14:03 EDT From milliken@BBN.COM Thu May 31 14:04:19 1990 Subject: Re: Debate on SJG raid in comp.risks

Re: Sherwood, RISKS-9.96:

To the best of my understanding, this account is correct except for trivial details (not a footlocker, but some filing cabinets were broken open in the account SJ himself wrote).

Re: Von Rospach, <u>RISKS-9.97</u>

> the person working on for Jackson Games was a former Legion of Doom member...

This first part of this also appears to be true -- Loyd was apparently associated with some bunch of crackers sometime in the past, and apparently

discussed some of the stuff he was doing with Cyberpunk with them, in the way of reality-checking. However, Cyberpunk was certainly *not* a "manual on hacking" -- I haven't read my copy yet, but I'm quite certain the game rules don't go into details of breaking computer security -- it just has abstract security programs and "cracking" programs as things that exist in the game world. These things also exist in cyberpunk novels, which is why they're in the book.

>If you're running a BBS that's supporting a group of system crackers, you are, >at least, contributory to felony crimes...

The problem was that SJG *was* clean, as far as I know -- the Secret Service just went overboard in their search for "contamination". I believe guilt-by-association is not a tenable legal theory in the US. Grounds for some amount of suspicion, yes. But search and seizure?

<>Or does it indicate that games which involve "hacking" are subject to ... >Not if the Legion of Doom angle is true....

The Legion of Doom connection appears to have been there, but very tenuous. The Feds seem to have been unable to draw the line between fantasy and reality, and appear to have been operating under a "guilty until proven innocent" premise as far as the seizure of equipment went. As far as I know, the Secret Service had no direct evidence that SJG or the BBS had *anything* to do with their case -- mere proximity to the principals seems to have triggered the raid. I would expect that they would have done more research before swooping down and carting off someone's business equipment.

I can understand how the raid happened, and even sympathize somewhat with the motivations of the Secret Service, but I think that they definitely stepped over the line here. One of the principles of the law in this country is that the innocent shouldn't be harmed in the pursuit of the guilty.

---Walter

RE:Steve Jackson Games

<EBB3840@SNYPLAVA.BITNET> Fri, 1 Jun 90 09:15 EST

The chance of GURPS Cyperpunk being used as a manual for computer crime is very slight indeed. In Cyperpunk fiction, a hacker's interface with the computer network he or she is trying to operate in is an actual physical connection with the computer. This connection is usually in the form of a direct link to a person's brain through jacks surgically implanted in their skull. It is my understanding that Steve Jackson Games used the same method of interfacing with computers in GURPS Cyperpunk. This would make it a little difficult for a person to use the game rules a handbook for crime. Unless they had a friend real handy with tools...:-).

Stephen J. Webb

Mailing list risks

John Chew <john@trigraph.uucp> Thu, 31 May 90 12:43:56 EDT

I received two copies of a well-known Macintosh software company's "Technical Solutions" newsletter today, identically addressed. It happens fairly often and I wouldn't have given it a second thought, except for the lead article: "Eliminate Duplicate Records: Omitting and Deleting Duplicate Records in

ATM range checking

ZENITH <ENITH@l66a.ladc.bull.com> Fri, 01 Jun 90 07:07 PDT

In <u>RISKS 9.96</u>, Richard Muirden writes of his experience with \$89m showing up in his bank account; his bank blamed him for keying in the amount at the ATM. He went on to wonder about the range checking that might or might not be employed at the ATM to catch "such obvious erroneous data". It is my experience that there is, indeed, NO such checking performed--at least at one institution, at one time.

A few years back, my credit union installed an ATM machine; as part of the hoopla surrounding the event, they had a demonstration where members could "practice" on the machine, using a card provided by the demonstator. I, being the obnoxious sort, made use of the opportunity to determine an empirical answer to the question of range checks. I cheerfully deposited the amount of \$99,999,999 in the account. The demonstrator was rather worried when I showed him the receipt (oops--I meant "transaction record"); it seems that they were using a live account for the demo, which meant that all these phoney transactions would show up on the balance sheets at the end of the day! I did hear later that the trouble caused was minimal, but they did have to jump through some hoops to make sure there were no ripple effects caused by that \$99m.

P.S.--My personal feeling is that any non-zero deposit is an "obviously erroneous value"; I don't like giving my money to a machine in exchange for a worthless transaction record. Andy



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Sat, 2 Jun 90 17:08:14 PDT

I was given this article by some colleagues who bought the magazine while visiting France for a research project meeting. Having had a quick look at it, I decided that it was *very* interesting. It contains chapter and verse on a couple of hair-raising incidents on board the A320, and the author obviously had access to the dossier of OEB's, from which he draws some fascinating conclusions regarding the general state of readiness of the A320 on entry into service and the possible causes of the Habsheim accident. He also includes an excellent summary of the legal wrangle surrounding the investigation into Habsheim. So, because of:

- a) the technical quality of the article,
- b) the fact that it presents a French (and therefore not negatively biased?) view, and
- c) the fact that it is not readily accessible to the majority of UK and US readers,

I decided, at *enormous* cost in time and effort :-), to make a careful translation of the whole article, and send it complete to RISKS and to Aeronautics Digest. [...]

LES CRISES DE NERFS DE L'A320

Translation of article by Bertrand Bonneau: Aeronautique, April 1990, pp. 94-101 [Translator's comments and additions are in square brackets.]

THE A320'S ATTACKS OF NERVES

- The first aircraft in the history of the world to be totally "managed" by
- computer; has the A320 been put into service before it is ready?
- The excessive number of incidents during its first year of use can only make
- one think so. How could the willingness to declare the pilots responsible for
- major accidents, even before the judges have returned their verdict, appear
- other than suspect? Even so, as everyone wished, the verdict whitewashed the
- aircraft.

At the start of 1988, the French authorities and Airbus Industrie congratulated themselves on the certification of the A320 only one year after the first flight of the prototype. In less than one year, the manufacturer had demonstrated the reliability of this new generation aircraft to the authorities of four of the States of the European Community.

However, controversy surrounding the aircraft would not be slow to surface at the time of the inaugural flight of the Air France A320, on 28th March 1988 over Paris, with the Prime Minister of the time on board. This flight was marked by a series of technical incidents, notably by the untimely setting off of alarms. New controversies were to arise when an aircraft was destroyed in the forest of Habsheim in Alsace (26th June 1988), and when an Indian Airlines A320 crashed before reaching the runway in Bangalore last February. In both of the last two cases, the aircraft was whitewashed as far as public opinion was concerned before the slightest preliminary accident report was published...

Although what have come to be called the "Chirac flight" and the "Habsheim affair" are the two facts most known to the public, the first year of operation of the A320 has been marked by numerous incidents which have directly called into question certain systems on the aeroplane. Often badly received by the first crews qualified on this aircraft, and sometimes vigorously denied by the technical directors of the launching companies, these incidents lead one to ask if the manufacturers and the certification authorities have not proceeded a little too quickly.

Twelve times more incidents than were foreseen. In his statement on the first year of operation of the A320 in the Air France fleet, a statement addressed to the general department of civil aviation (Direction Generale de l'Aviation Civile - DGAC) on the 11th July 1989, the technical sub-director of operations management of the national company remarks that the first exercise has been marked by "a greatly increased number of technical incidents altogether" (page 12). Whereas the target set was one incident per thousand hours of flight, the year 1988 ended with an incident rate of twelve per thousand hours of flight. For comparison, this rate was 5/1 000 at the time of the first year of operation of the Airbus A300.

The frequency of these incidents which have marked the A320 going into service within Air France, Air Inter and British Airways has forced the manufacturer to publish no fewer than 52 provisional flight notices (OEB, Operations Engineering Bulletin) between April 1988 and April 1989. The launch of a new aircraft requires on average four times fewer. OEB's are temporary notices sent out by the manufacturer to the users. They form a list of anomalies or simply functional features of the aircraft, which do not appear in the users' manual for the equipment (FCOM, Flight Crew Operation Manual): they are only revealed

in the course of operation. In the case of Air France, these provisional records are provided to the crews in the form of a volume of supplementary technical information notices (Renseignements Complementaires Techniques - RCT's).

For the A320, the number of OEB's alone gives an account of the problems of putting the aircraft into service. At the technical level, around twenty of the fifty main computers of the first A320's coming off the production lines in Toulouse have had to undergo modifications. For the A320 is the first aircraft in the world to be completely computerised. Computers control the function of all the systems of the aeroplane (motors, ailerons, but also the cabin lighting, etc.); it [sic] processes raw data, converts them, and transmits them to the pilot. Now, the application of numerous modifications defined by the manufacturer in order to correct defects in the systems or to enhance them, has been the origin of new breakdowns. These new problems have obliged the manufacturer to publish new OEB's before drawing up final modifications.

During service, companies have had to modify once or several times certain procedures for operating their aircraft. Also, with the exception of Air Inter, which reported only good results, the increased number of incidents was the origin of poor availability and bad technical readiness of the first A320's delivered. "Of 7 334 stop-overs [landing + take-off's (?)] carried out up to April 1989," states the report of the technical sub-director of Air-France, "one lists on technical grounds [i.e. something went wrong (?)]: 4 accelerations-stops on take-off, 36 about-turns on the ground, 10 about-turns in the air, 1 emergency descent procedure, the cabin altitude being on the increase (without violent decompression), 1 engine stop in flight." [If you think this lot is confusing, you should see the original French! I think an about-turn on the ground is an aborted take-off, and an about-turn in the air is a return to the departure port. I'm not sure what the difference is between an about-turn on the ground and an acceleration-stop. Presumably the latter means the engines raced or cut-out during approach to take-off. 'Cabin *altitude* being on the increase' is a literal translation: I think it means the cabin atmosphere was below pressure, since they came *down*. Anyone with access to a dictionary of French avionic terms, or who knows the correct English avionic terms is welcome to correct me!] It is advisable to add to these outcomes the grounding of aircraft due to suspect behaviour, and 74 cancellations of flight before even starting up the engines.

Reliability in question. For the aviation companies, the most serious problem would seem to have been that of the reliability of the information given to the crew by the various systems of the A320. The operating assessment by the technical sub-director of Air France is edifying on this subject. One discovers there, for example, that: "certain inconsistencies of piloting information have led to certain confused and very distracting situations, where the information presented to the pilots on the control screens, during flight, was in contradiction to the physical reality of the equipment, not always verifiable in flight", (report already cited, page 18). [Presumably this means: "The instruments were lying, but the pilots couldn't get out and walk around to check this at 30 000 feet!" Nice to know that French technical officialese is as obscure as British or American! ;-}]

Without a doubt, Captain Claude Dalloz and First Officer Patrick Vacquand share the views of the technical sub-director of Air France. On the 25th August 1988, while taking off from Roissy on a flight to Amsterdam (flight AF 914), they had the disagreeable surprise of seeing the message "Man pitch trim only" appear in red on their control screens. In plain terms, this message informed the pilots that the controls activating the pitch control mechanism were no longer in a functional state. In this case, the only means of ensuring the longitudinal stability of the aircraft is to manually move the trimmable horizontal stabiliser by means of the pitch trim wheels.

Meanwhile, the copilot who was at the controls felt not the slightest difficulty in controlling the aircraft. Then the crew witnessed a display of imaginary alarms ("fire in the toilets", for example), and noticed new signalling anomalies on the screens concerning the flight control systems, the position of the landing gear, and also the situation of the automatic pilot.

It was therefore decided to return, but, during the approach, the gear at first refused to come down normally. Given the uncertainty, three passes at low altitude were made in front of the control tower to ascertain the real position of the gear after having carried out safety manoeuvres. As the information provided to the crew ("gear partially down") did not correspond to the observations of the controllers at Roissy (gear down), the passenger cabin was prepared for an eventual crash, which did not, very fortunately, occur. The same incident recurred on another plane on 29th November 1988. It finally required nine months of operation before a new, more reliable, version of the Flight Warning Computer (FWC) called into question by these two cases was made available to users.

A temperamental altimeter. A good many problems due to the design of certain systems have revealed themselves since the start of operation. The most spectacular, for the passengers, would have been the vagaries of the integrated cabin communication system (CIDS), which modified explanations or illuminating announcements in an eccentric fashion. More seriously, the crews discovered that the temperature regulation of the passenger cabin could interfere with the functioning of the engine power control computers (FADEC), generating breakdowns and alarms. To avoid these interferences, crews were asked not to "reinitialise" the cabin temperature regulation system while the engines were running.

However, the most worrying phenomenon for the crews has been the untimely alterations to the setting of the altimeters during flight. Having reached a certain altitude, the pilots set their altimeters in a standard way, calculated in relation to the theoretical atmospheric pressure at sea level (1 013 hPa), in order that all aircraft using the airspace should have the same reference for altitude (QNH base). Relative to this base, the altimeter indicates a pressure altitude, which is a "QNE" altitude. While the aircraft is descending, at a predetermined height the crew must set their altimeters in relation to the altitude of the destination airport (QFE base). Apart from some very rare landing strips situated below sea-level, airports are above this [sea-] level. Since pressure diminishes with altitude, the value of QFE is generally less than 1 013 hPa. The sudden alteration of the altimeter setting by the flight programming computer (FCU, Flight Control Unit) sometimes occurs in uncomfortable conditions. So, in July 1988, during an approach to Roissy,

the untimely alteration of the altimetric setting, which conveyed itself as a reversal of the altimeter reading, provoked an automatic delivery of fuel in order to compensate for the false deviation in altitude generated by the defaulting computer and detected automatically by the safety systems of the aircraft. This delivery of fuel occurred while the aircraft was being flown manually on its descent. The rapid intervention of the pilot could not avoid the aircraft going into overdrive for several seconds.

Untimely alterations of altimetric settings showed up on at least the first three planes delivered to Air France, among them the aircraft which crashed at Habsheim. The commission of enquiry has revealed in its final report that such an incident had taken place on the plane several hours before its crash, concluding immediately that this anomaly due to a design error had played no part at all in the accident. Moreover, the flight report (CRM, compte-rendu materiel) of a crew, concerning a third aircraft of Air France, made mention of vagaries of the altimeter.

It is therefore surprising that the report of the technical sub-director of Air France limits this type of incident to a single A320 of his fleet (the aircraft registered F-GFKB), when it has also occurred on at least two other planes (registered F-GFKA and F-GFKC). But the most amazing thing remains that this functional anomaly should cease without anyone being able to identify its origin!

Recording of parameters. In an indirect manner, these two types of incidents have revealed another potential source of problems in the level of the recording of parameters by the "black box recorder" (DFDR, Digital Flight Data Recorder). In effect, each piece of information given to the pilot is handled by a cascade of computers. Now, this "black box" records the majority of its information on the intermediate computers and not at the start or end of the processing chain. When examining this data, therefore, there is nothing that allows one to know precisely what the pilots had for information, since there is no recording at the output of the symbol generator [DMC] for their screens.

The problems posed by the flight data recording system can be illustrated by referring to the two incidents mentioned. If the Paris/Amsterdam flight recalled above had ended in a crash, the "black box recorder", which captures a large part of its information from the flight warning computer (FWC), would have revealed that the crew no longer had pitch control available. In fact, all the flight controls were functioning, but the flight warning computer, which is one of the principal sources of information of the "black box recorder", had failed (diagram, p.98).

Equally, if the untimely alterations of the altimeter readings had ended in a crash, the "black box recorder" would have revealed no malfunction of the altimeter assembly, since the recording of pressure altitudes (QNE), which was correct, is effected by equipment located upstream of the failing computer. This computer (FCU) incorrectly processed the information which had been sent to it, and an erroneous indication of altitude was sent to the control screens (diagram above, p. 99).

Modification Campaigns. Before the A320's went into service, the launch

companies' instructors - who cannot be accused of bias since they were all volunteers - complained of having had no contact with the test pilots of Airbus Industrie. The report of the technical subdirector of Air France, for its part, confirms this worry by revealing that it had at last been possible to establish a "frank relationship" (page 17) after six months. The adaptation of failing systems has been progressively integrated in the course of several modification campaigns begun at the start and middle of 1989 as problems were found and listed. It was necessary to wait until the end of last year to obtain the definitive version of certain pieces of equipment, that is to say, eighteen months after the certification and entry into commercial service of the A320.

At the end of last year, the dossier of supplementary technical notices (RCT's) distributed to A320 crews already comprised eleven pages, whereas the RCT's of other aircraft in the Air France fleet rarely got beyond three pages.

Contrary to the fears expressed many times in the course of these last years, not only by certain pilots' unions, but also by the American certification authorities (FAA, Federal Aviation Authority), the electrical flight controls and the electronic engine control system, which constitute the two great technological innovations of the A320, would never be the direct cause of any significant incident, notably in stormy conditions. During test just as in service, the A320 was struck by lightning several times without the least influence on the flight controls.

The majority of the teething troubles and design faults of the A320 therefore concern more classical systems. The report of the technical sub-director of Air France is once again definitive: "Pressurisation, management of cabin communications (CIDS), pneumatic generation, auxiliary power units (APU)... have been for a long time of an unacceptable reliability. Everything is still not under control to this day (NDLR: 11th July 1989)." (Report already cited, page 17).

Industrial secret. It could therefore be thought that the certificator has turned his attention above all to the innovative elements (flight controls, FADEC, etc.) of the A320. However, this explanation, although not completely without foundation, does not take into account the fact that the systems called classical are also subject to major innovations, since they practically all require computer automation.

Without invoking the young demons of computing, the embedding of numerous pieces of software on board aircraft of the new generation (A320, but also McDonnell-Douglas MD 11, Boeing 747-400, among others) can pose problems for the official agencies. Up until then, the certificators were confronted by much more simple systems (cabling, for example) and by perfectly mastered technologies (electricity, for example). With the A320, the certificator found himself before a gigantic interactive data processing system, made up of "boxes" which consisted of inputs and outputs. No-one having foreseen such a rapid installation of computers on board service aircraft, it was not possible to find, in the international regulations, standards directly applicable to this domain.

Furthermore, the certificator came up against protection of embedded software by industrial secret. The official agencies were finally forced sometimes to

give their agreement to a piece of equipment, on a simple demonstration of the required result, without being able to know precisely the organisation of the system which allowed it to be reached. In such a context, only a more thorough programme of tests would have permitted the major design faults of certain systems to be revealed with certainty and would have avoided certain launch companies having to proceed with the modification of nearly half of the main computers of their first A320's.

The protection of software by industrial secret constitutes a source of problems also for the users' maintenance services, who must leave it to the manufacturer to understand the reasons for its failure. For the time being, the best equipped companies are provided with certain software test sets, but eventually the users will have to be able to test their systems directly on the battery of test sets of the manufacturer through data transmission networks.

The dead-ends of certification. It is interesting to note that use has revealed several loopholes in certification. A provisional information bulletin dating from the month of May 1988 (OEB no. 06/2) reveals for example that the single information source for the pilot's and copilot's altimeters on the A320, is not compatible with certification standards [i.e. it makes a single point failure possible?].

Another provisional information bulletin sent out in August 1988 (OEB no. 33/1) indicates that the safety lighting system of the floor of the passenger cabin does not conform to certification standards. This system would not automatically illuminate when one of the emergency evacuation devices of the aircraft was activated, in the case of the loss of the normal electricity supply. Now, this lighting system provides an illuminated pathway in the central aisle of the cabin, which must allow passengers to find the safety exits or doors during an evacuation in the dark or in smoke. This design defect was underlined by the final report of the commission of enquiry into the Habsheim accident.

"To be the launch client of a new aircraft is sometimes a painful task," one of the directors of Air France confided last year, before adding that "the A320 would attain the level of reliability of the fleet (of Air France) by the start of 1990." This would be practically two years after the certification of the aircraft. A last example: it has been necessary to wait until the month of July 1989 for it to be noticed, in the course of a test flight, that the landing gear could, in certain cases, not retract fully in case of a shut-down of engine no. 1 during take-off (OEB no. 62/1). (1)

The totality of these elements, then, could allow one to believe that speed and haste had been confused.

Bertrand Bonneau

-----[Footnote:]

(1) The OEB's are intended to be temporary. As a consequence, the anomalies with which they are concerned when they are sent out, have normally been corrected.

[End of main article. Text in boxes accompanying illustrations follows:]

[Box on p. 95, below photograph of cockpit:]

Up to the customer to complete the tests. The standards and certification procedures of civil aircraft are not adapted to the A320, an aircraft which, for the first time in the history of civil aviation, is massively equipped with data processing systems. For example, the software in the flight warning computer [FWC] included a fault which a good computer scientist could have repaired without a doubt. But this software is protected by industrial secret, and as luck would have it the fault did not show itself at the time of the certification campaign. Result: an aircraft has been sold with a certain number of latent defects, which the first customers have discovered bit by bit.

[Box on p. 97, accompanying photographs of instrument panels in cockpits of (1) A320, (2) A310, (3) A300:]

THE TECHNOLOGICAL LEAPS OF THE AIRBUS

The A320 (1) is the first aircraft whose cockpit panel is entirely equipped with cathode tube screens [CRT's]. Only three traditional instruments are still found there, in case of failure of the former [i.e. CRT's]. The new screens display more synthetic and more complete information to the crew. So, the whole navigation of the flight is directly visible to one of them, and the image evolves in real time along with the movement of the aircraft, whereas on traditional aircraft, this tracking is effected by the pilot on a piece of paper on which he reports the successive positions given by the on-board equipment (radiobeacon receiver, radiocompass, inertial platform [IRS?], etc.). But these screens can also, unfortunately, deliver erroneous information if one of the systems that supplies them is failing; and the irony is that often this information cannot be verified by the pilots in flight (see diagrams, p.98). An aircraft of the preceding generation, the A310 (2), was already equipped with some screens, whereas the A300 (3), which was developed at the start of the 70's, is only equipped with classical electromechanical instruments.

[Box on pp. 98-99, illustrating two incidents described in the main text, labelled case A and case B in the boxed text to allow cross-reference between that and the two accompanying diagrams, which show by numbered labels the placing, and communication between, the following:]

- 1. PFD. Piloting screen. It is this which displayed "manual pitch trim only" in case A in the text, and the erroneous QFE altitude in case B.
- 2. ECAM. Screen which gives information about the aircraft systems (motors, lighting, etc.).
- 3. PA. Automatic Pilot.

- 4. Side-stick.
- 5. FCU. Flight Control Unit.
- 6. DMC. Symbol generator for screen displays [Display Management Computer].
- 7. SEC-ELAC-FAC. Computer [sic] for flight controls (ailerons, pitch control surface, flaps, spoilers, etc.).
- 8. ADIRU. Air Data Inertial Reference Unit
- 9. SDAC. System Data Acquisition Concentrator, which translates into data processing language the data received from systems upstream of it (sensors, controls, etc.).
- 10. FDIU. [Flight Data Interface Unit] Computer for the flight data recording system, which manages the "black box recorder" [DFDR].
- 11. Hydraulic servo-mechanism for pitch control surface.
- 12. Trimmable Horizontal Stabiliser [THS] and pitch control surface.
- 13. DFDR. "Black box recorder" [Digital Flight Data Recorder].
- 14. Switch for display of QFE pressure [on FCU]

BREAKDOWNS AND DANGERS INVENTED BY THE COMPUTER

A. Alarmist computers. This simplified diagram [p. 98] of the A320 systems (which takes no account of the actual location of the computers) shows how the crew of flight AF 914 of 25th August 1988 found themselves confronted by nonsensical information generated by the flight warning computer (FWC). This sent the erroneous message "manual pitch trim only" to the piloting screen (PFD) and to the "black box recorder" (DFDR), a message informing of a loss of control of the pitch control surfaces (red arrows). [Sorry. Colour diagrams are difficult over e-mail ;-)] Put simply, the pilot can no longer control the climb or descent of his aircraft with the stick (but only by means of a manual back-up control). In fact (green arrows), this control [i.e. the electronic one] was functioning perfectly.

B. Imaginary altitude. The second diagram [p. 99] shows how the pilots had on their screens an untimely alteration to their altimetric setting, generated by the flight control unit (FCU), whereas the altitude data in the air data inertial reference unit (ADIRU) was correct. The FCU prompted an inversion between the pressure altitude (QNE) and the altitude of the destination landing strip (QFE). As the QFE was giving an altitude below the QNE altitude (which would allow one to believe that the aircraft was flying dangerously lower than it was in reality), the safety systems of the aircraft demanded an automatic delivery of fuel to regain height. [Box on pp. 100-101:]

HABSHEIM ACCIDENT: CFMI ASSESSES CFMI

On the 26th June 1988, the air show organised by the little flying club of Habsheim, in the Haut-Rhin, turned to drama when an Air France A320 crashed with 130 passengers in the forest which bordered the landing field, in the course of its display flight. In a few minutes, the aircraft was almost completely burned. Toll: 3 dead, 34 injured, the other 93 occupants unhurt.

Nearly 18 months after the accident, the Commission of enquiry delivered its report. Contrary to what it had been possible to affirm, this document (called the "Bechet report" after the name of the president of that commission) does not establish any responsibility, but limits itself to stating the facts and suggesting some measures. After all, only judges are entitled to decide blame and responsibility. Now, this decision has not taken place. The investigating magistrate has even requested recently the reopening of the inquiry for supplementary information.

No-one knows, then, what the Mulhouse magistrate thinks, but the context in which the enquiry into this accident was begun could be marked by certain irregularities. Indeed, on the evening of the drama, the director general of Civil Aviation was filmed by a television crew as he took charge of the transport of the two "black boxes" (CVR and DFDR). Now these two recorders are the essential elements for the enquiry. The presence of the director general of civil Aviation at the scene of the accident and the particularly active role that he played that evening seem hardly compatible with the ministerial directive of the 3rd January 1953 relating to the coordination of the judicial inquiry and the technical investigation and with directive no. 300 IGAC/SA of the 3rd June 1957 concerning the steps to be taken in case of irregularity, incident or accident in aviation. The General Directorate of Civil Aviation having had the responsibility of certifying the aircraft and having authorised the holding of the meeting, it is legitimate to ask oneself if its director is not simultaneously judge and party to the case. Moreover, the authority designated by the regulations as being competent in the matter of enquiries is not the DGAC but the General Inspectorate of Civil Aviation (IGAC), placed under the direct authority of the Minister of Transport.

A second factor, which follows from the first, could leave one to suspect that the concern of the only technical enquiry had overridden that of the judicial enquiry. First, it was necessary to wait two days for an investigating judge to be appointed, whereas that is generally done in half a day for major accidents; and this is one of them [i.e. major], with, moreover, a considerable amount at stake. Furthermore, the two black boxes were left for nine days without any judicial control, since the placing under seal was only done on the 5th July (let us recall that the accident took place on 26th June). In the meantime, parts of the recording of the conversations held in the cockpit during the flight were published in the press, in defiance of the secrecy required by the directive [i.e. no. 300 IGAC/SA of 3rd June 1957(?)].

Reading of the Bechet report (page 41) reveals that the assessment of the

damaged aircraft engines was entrusted to their own manufacturer (CFMI), on the SNECMA premises at Melun-Villaroche. Without casting doubt on the quality of the assessment achieved by the manufacturer on the premises of one of his partners with the participation of the Commission of Enquiry, it seems astonishing that the manufacturer should have had control over a procedure which concerned him so directly. As one knows, in the case of an enquiry relating to an accident, an assessment is always likely to have judicial consequences.

That is all the more surprising since the engines had been directly implicated by the statements of the crew immediately after the accident. One can therefore ask oneself why the assessment of the two CFM56-5A1's was not entrusted to the experts of the Propeller Test Centre of Saclay, which comes under the Flight Test Centre. Indeed, this centre does not have any judicial, industrial or commercial links with the equipment in question.

Even if the conclusions of the commission of enquiry, based on that assessment and on the recording of the "black box recorder" [DFDR], categorically rule out the two engines, that will not cut short some of the objections which some of the lawyers would have been able to try to set out before the judges of Mulhouse. Such would not have been the case if that investigation had been entrusted to an organisation which was not also an interested party.

If the defects of acceleration of the CFM56-5A1 engines of the Air France A320, noticed sometimes in certain cases of low altitude flight, did not exhibit themselves at the time of the accident, why, then, was a provisional information bulletin (OEB 19/1) sent out in May 1988, modified in the following August (OEB 19/2)? Moreover, the adjustment of the stator blades (counterbalancing [?] of the jacks which modify their pitch [?]) of these engines, which has a direct link with their efficiency at low speed and at low altitude, was also modified a short time after the accident. There again, why?

DISCLAIMER:

- 1. The opinions expressed in this article are not necessarily the opinions of City University, of the Centre for Software Reliability, or of the translator.
- 2. Misprints in the original are the responsibility of the publisher.
- 3. Factual errors in the original are the responsibility of the author.
- 4. Errors in translation are the responsibility of my O-level French mistress.
- 5. I am not responsible for ANYTHING! ;-}

Peter Mellor



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<iwm@doc.imperial.ac.uk> Fri, 1 Jun 90 17:55:40 BST

This is a summary of an article in the Guardian for 1st June: `Computer hitch stalls GP budgets', any inaccuracies are mine.

At the moment UK family doctors are funded according to the size of their practice and various overheads. As part of changes to the National Health

Service, doctors may be required to maintain their own budgets and buy treatment from local hospitals. To do this doctors will require specialist software to interface with hospital databases as well as doing their own accounting. The first stage of the scheme involving several hundred doctors was to start next April. The changes are unpopular and doctors are dropping out, software firms working in the area claim that developing the software is not worthwhile given the number of sales to those doctors participating. It was stated that even if the government funded the development there is not enough time to produce and test the software in time.

Although it is not stated in the article, I believe that one problem may be that different hospitals run different (and incompatible) accounting software.

Ian W Moor JANET: iwm@uk.ac.ic.doc Department of Computing, Imperial College. 180 Queensgate London SW7 UK.

Ke: Airline Booking Cancellation (<u>Risks 9.91</u>)

Pete Mellor <pm@cs.city.ac.uk> Sat, 2 Jun 90 18:53:19 PDT

I have been asked for the full reference to the paper I referred to in the above article. It is:

Adam R: "A licence to steal? The growth and development of airline information systems"
Journal of Information Science 16 (1990), pp. 77-91, 0165-5515/90/\$3.50, Elsevier Science Publishers B.V.

Apologies to anyone who had difficulty tracking it down. I will snail photocopies if requested.

Peter Mellor

Hacking, Viruses, and UK Law

Pete Mellor <pm@cs.city.ac.uk> Sat, 2 Jun 90 21:41:40 PDT

Recent raids on suspected hackers and the likelihood of anti-virus legislation in the US (<u>RISKS 9.95</u>) should not make us forget what is happening in the UK.

The story so far:

In September 1988, the English Law Commission (ELC) issued a consultative document, "Computer Misuse".

In April '89, Emma Nicholson, MP, proposed a private member's bill to make various hacking activities illegal. This was generally thought to be poorly researched, and too hastily drafted. It was roundly attacked in the Guardian by, among others, Peter Sommer (aka Hugo Cornwall, author of "The Hacker's

Handbook). The bill failed for lack of time. (A frequent fate of private members' bills.) [1]

In October 1989, the ELC published its final report on "Computer Misuse" [2]. This suggested three new offences. I quote from a summary by Peter Casey of the DTI [3]:

- a basic offence which will apply to anyone who seeks to enter a computer system knowing that the entry is unauthorised. This would be punishable by up to three months imprisonment.
- a more serious offence of unauthorised entry into a computer system with intent to commit or assist the commission of a serious crime. This would be punishable by up to five years imprisonment.
- a further offence of intentionally and without authority altering computer held data or programs, punishable with up to five years imprisonment.

Because of the international nature of computer misuse the Commission also proposes reform of the jurisdiction rules to remedy a gap in the current law whereby an offender initiating or furthering a crime completed abroad may escape prosecution in any country. [End of quote.]

Another private member's bill implementing these proposals was introduced by Michael Colvin, MP, and received its 2nd reading in the Commons on May 4th 1990. Called the "Computer Misuse Bill", it has been amended to allow powers of search and entry of suspected hackers' premises by police armed with a magistrate's warrant. It passed its second reading with the amendment, but without stronger amendments proposed by Emma Nicholson "to give magistrates powers to sign warrants that extended that extended the police powers of search and seizure, and for judges to sign warrants that allowed the police to intercept computer communications....She pressed for an amendment that would oblige British Telecom and Mercury, on the instructions of a magistrate, to begin surveillance of designated communications traffic."[4]

The bill was attacked by Harry Cohen, MP. "The first major problem raised by Cohen was that the bill doesn't define the term 'computer'. He also questioned how the offence of 'unauthorised access' would be applied in practice. Cohen pointed out that the lack of a definition raises the spectre of unauthorised access to the microchip computers found in 'domestic appliances such as a sewing machine with a programmable pattern, or a washing machine, video recorder or compact disc player that can be programmed'. Even fax machines or photocopiers would lead to some 'farcical prosecutions', he asserted. However, other anomalies would arise if a definition of 'computer' were included. For example, if a computer were described in precise and exacting terms, would the next technological development produce a computer that was not a computer as defined by the Computer Misuse Bill?...In the end, it was decided not to include a definition of computer in the bill, as this would let the courts decide in each case." [4]

Cohen's second attack was more interesting. "...Cohen drafted three amendments to ensure that the security procedures adopted by a computer owner could be examined by the courts....if computer owners did not have security procedures that sufficiently protected their computers from unauthorised access, the hacker could get off. [From the basic charge of unauthorised access.] Cohen's other two attempts were variants aimed at extending the Data Protection Act to all computer operations. The MP argued that any individual who suffered damage because computers, software or data were insecure or unreliable, should be able to seek compensation from the owner via the courts or the data protection registrar. The owners would have one main defence: to show that they 'had taken such care in all circumstances as was reasonably required' to maintain the reliability and security of the computer, data or program in question."[4]

(His amendments failed.)

The main arguments can be summarised as:

Cohen (quoting Francis Aldhouse, deputy data protection registrar) [4] : "You've only yourself to blame if your neighbour's cattle get into your unfenced field.", and:

"Logic dictates that computer owners should be legally responsible for the security of their computers just as gun owners are responsible for their guns."

Nicholson [4]: "If a madman with a knife attacks another person in the street, would the victim be responsible for not taking reasonable care to prevent the attack?"

Sommer (arguing against Nicholson) [1]: "In fact, most of the computer-related activities most people would think ought to be criminally sactioned already are."

It will come as no surprise to UK readers to learn that Colvin and Nicholson are Conservative, and Cohen is Labour, and that the government are being supportive in such little matters as parliamentary time.

Interestingly, Colvin seems to favour some of Cohen's arguments. Speaking at a contingency planning and disaster recovery seminar, he said: "If companies do not invest in their own computer security strategy, then they cannot expect the sympathy of the courts when people are charged under the provisions proposed in my Bill." [5]

Also, Nicholson "plans to introduce a Computer Usage Bill in the autumn, which will lay down rules for the use of computers covering maintenance, support and upgrades." [5]

The truth of Sommer's argument is illustrated by the case of one Nicholas Whiteley, appearing before Southwark Crown Court last week on seven charges of criminal damage arising from hacks carried out during six months in 1988. He admits the hacks, but claims he did no damage. (My private information is that he overwrote files with joke messages, and the amount of damage was estimated as &25 000. I also believe he was convicted, but haven't seen a report of his sentence.) He hacked ICL series 39 machines at Queen Mary College, Hull University, and Glasgow University. He told the court: "My messages weren't a threat, they were just a wind-up." [6]

The Computer Misuse Bill, in the meantime, goes on to committee and then to the

Lords, then back to the Commons. If it succeeds, we should start worrying about just how 'authorised' we are around September.

References:

[1] Hugo Cornwall: "Wrong ways on hacking", Guardian, 13th April 1989.

- [2] The Law Commission report, Command 819, Criminal Law, Computer Misuse, (Law Com. 186), HMSO, &5.60
- [3] Peter Casey: "Proposals to curb computer misuse", JFIT News, Issue 8, Nov. 1989, Pub. DTI/SERC
- [4] Chris Robbins: "Hacking through both the Houses", Computing, 24th May 1990
- [5] Lindsay Nicolle: "No sympathy for security slackers", Computer Weekly, 24th May 1990
- [6] Tony Collins: "Hacker exposes security of university systems", Computer Weekly, 24th May 1990

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V OHB Tel.: +44 (0)71-253-4399 Ext. 4162/3/1

Ke: ATM range-checking (<u>RISKS-10.01</u>)

Jim Horning <horning@src.dec.com> 1 Jun 1990 1336-PDT (Friday)

It's pretty clear that different banks have different practices, as well as diverse equipment. My bank (Wells Fargo) advertises that they will credit you with an extra \$10 if the ATM makes any mistake on a deposit (and, indeed, I've never detected one). They also do some range-checking. I haven't conducted extensive experiments, but I recently deposited a check for an order of magnitude more than my usual deposit, and was asked to confirm an extra time before the transaction was completed. I thought that this was a very sensible precaution.

In a related vein: When I first got my ATM card it was limited to \$200/day of cash withdrawal, which is not unreasonable. However, after a decade of modest inflation, there were times (like just before trips) when a larger sum would have been convenient. One day it occurred to me to try to withdraw more, and what do you know? It disbursed \$300 without complaint. So my trips to the ATM became less frequent. Some time later, I noticed that years of carrying the card in my wallet had cracked it, right across the magnetic stripe. So I asked for a new one. Now I'm limited to \$200/day again. I infer that it was a fault on the stripe that let me withdraw more. I would have hoped that the limit was enforced by something less subject to decay and/or tampering.

Jim H.

Re: Debate on SJG raid in comp.risks

That's MR. Idiot to you <chuq@Apple.COM> 1 Jun 90 18:37:35 GMT

Just to clarify one thing:

<>If you're running a BBS that's supporting a group of system crackers, you are, <>at least, contributory to felony crimes...

>The problem was that SJG *was* clean, as far as I know -- the Secret
>Service just went overboard in their search for "contamination". I
>believe guilt-by-association is not a tenable legal theory in the US.

A couple of people have taken my comment above as implying I think that SJG was running a cracker board. Not true. From everything I've heard they are definitely in the "innocent bystander" category. Why haven't they got their stuff back? Very good question. All I'm hearing on my side is variations of "it ain't over until it's over" -- which to me sounds silly based on what I know.

I am definitely NOT trying to justify the impounding of SJG stuff, nor attempting to imply guilt or anything else at them. I was simply pointing out that the situation was more complex than some were making it out to be. The Secret Service seems to have good cause to talk to SJG about this stuff? Yes? Did they need to go in and grab all the gear? From what I know, no -but I don't know all the details of the case. The details I do know indicate they over-reacted, however.

Chuq Von Rospach <+> chuq@apple.com <+> [This is myself speaking]

Ke: 2600 article

Kee Hinckley <nazgul@alphalpha.com> Fri, 1 Jun 90 10:51:55 EDT

Please someone correct me if I'm wrong, but I think there's a Catch 22 here.

The evidence suggests that I can be arrested based on the contents/usage of my BBS, even when I'm unaware of that usage. (It remains to be seen whether I can be convicted, but frankly, if my equipment gets confiscated for a couple years, I hardly care.)

However, it seems to me that the Electronic Privacy Act prevents me from taking any actions which would let me prevent the misuse of my board. Namely, I can't read people's mail/files to see if they are doing something illegal.

Is this really the case? -kee

Alphalpha Software, Inc., 148 Scituate St., Arlington, MA 02174

Ke: Steve Jackson Games and A.B. 3280 (Von Rospach, 9.97)

ZENITH <ENITH@l66a.ladc.bull.com> Fri, 01 Jun 90 11:17 PDT

Chuq Von Rospach (chuq@apples.com) writes:

If you're running a BBS that's supporting a group of system crackers, you are, at least, contributory to felony crimes.

By law? Why? We don't hold a package delivery service like UPS liable

if they happen to deliver burglary tools; why is the owner/operator of a BBS treated differently for what seems to me an equivalent offense? Von Rospach goes on to say:

A BBS that's on the up-and-up should have no worries, though.

That seems to be the central issue; it shouldn't be tossed off so casually. The Bill of Rights is predicated on the assumption that the innocent have a legitimate reason to worry about the effects of actions taken by their government; governments to that point (and since) had not been terribly worried about who got chewed up by the wheels of justice, so long as some "guilty" party was convicted. Human nature has not changed much in the intervening years--there are still those who hold to the creed of "Kill 'em all; let God sort them out". We the innocent still need protection from those who would elevate expedience over justice; if ease of implementation and administration becomes the primary criterion by which we judge our laws, we are in deep trouble.

I have noticed a disturbing trend in society, towards a belief that it is better that 100 innocents should suffer than one guilty critter should go free; it is difficult to reconcile this notion with that of "innocent until proven guilty".

- Andy -

Kisks of moderated newsgroups and COWABUNGA

Nathan K. Meyers <nathanm@hpcvxnkm.cv.hp.com> Fri, 1 Jun 90 12:01:46 pdt

By now, most readers of moderated newsgroups on the internet have had the pleasure of reading the semi-literate ramblings of "THE BIFFSTER". As best I can tell, the following has been shown by this exercise:

- 1) Moderated newsgroups are not particularly secure (did anyone think otherwise?).
- 2) You can make something foolproof, but you can't make it damn foolproof.

- 3) The perpetrator may have reached a new world record in the irr/eff ratio (irr = number of people irritated, eff = effort expended).
- 4) Gone forever are the days when breakins were conducted by individuals with above-average intelligence and sense of humor (remember moskvax!kremvax!chernenko many Aprils ago?).

Nathan Meyers

[RISKS has spared you all the gory details of this case, which have been so widespread that it did not seem necessary. PGN]

Computer to track down drivers without insurance

<wex@pws.bull.com> Fri, 1 Jun 90 16:22:10 edt

The following is excerpted from a UPI newswire story:

BOSTON (UPI) -- Tens of thousands of illegally uninsured drivers in Massachusetts will be tracked down and hunted when the Registry of Motor Vehicles implements a new computer-based system beginning Friday [6/1/90].

The new system, which allows insurance companies to electronically send the Registry's computer a list of uninsured motorists whose policies have been revoked for nonpayment, aims at cracking down on the estimated 300,000 Massachusetts drivers who take to the roads without insurance.

"Hopefully with automation, deadbeats who don't have the money or those who try to beat they system won't be on the road," said Robert Hutchinson, Massachusetts registrar of motor vehicles.

Police will pursue those individuals who fail to obtain insurance after being discovered.

[Generic filler about the costs of uninsured motorists - sky-high and the hope that the computer will do what the people are unable to do: keep up with the workload.]

The significance of this is that there is a new law in MA: get caught driving without insurance and the cops can take away your license plates on the spot. You then get to call a tow truck, since you can't drive without plates. Get caught driving without plates and you get to call a cab, since the cops can have your car towed on the spot.

The problem is that insurance companies in this state are notoriously slow in processing paperwork. That's a major reason why so many uninsured motorists get away with it; the paperwork just hasn't caught up with them.

The companies take this long with *all* their paperwork. My company took four months to send me a reinstatement notice after they (erroneously) suspended my insurance for not having the car inspected (though they continued to bill me every month). I shudder to think what would have happened had I been stopped during those four months...

--Alan Wexelblat, Bull Worldwide Information Systems phone: (508) 671-7485 Usenet: spdcc.com!know!wex

✓ Local solution to caller ID .vs. Privacy problem

"FIDLER::ESTELL" <estell%fidler.decnet@scfd.nwc.navy.mil> 1 Jun 90 13:34:00 PDT

The following is by definition going into the Public Domain. (If RISKS posts it.) If that costs me any chance to make a fortune from AT&T, maybe it also raises the possibility that the solution will come sooner.

Problem: Some of us want to know "who is calling." BUT some of us don't want others to know when WE call.

Solution: Put the smarts for "who are you?" and "none of your business" [or, "I'm 555-1234"] in the handsets, at each end, NOT in the switch [or switches, for long distance calls].

Old handsets would automatically neither request caller ID, nor give it. Folks who want to know would buy new handsets; when they get calls from old handsets, the reply to the "who are you?" query would be, "service not available" [as opposed to "none of your business"]. Yes, a smart switch would have to provide that, probably after a time-out of sorts; and yes, that could be spoofed. Nothing is perfect. (But wait. Could even an old handset, touchtone or rotary, reply manually to a ring, while the line was open? That is, I call you, and you want to know who I am; your query is forwarded to my old handset as a ring; to send you my number, I dial it; the intermediate switch aborts the call, with an appropriate message to you, if it detects my attempt to falsify my ID.)

It is then up to the callee to accept or decline the incoming call; and, it is up to the caller to risk losing the connection. That effectively takes the decisions out of the hands of big brother, and puts them back with us, where they belong.

Bob

Ke: Denial of service due to switch misconfiguration

John R. Levine <johnl@esegue.segue.boston.ma.us> 1 Jun 90 18:33:46 EDT (Fri)

In every PBX I have ever dealt with, there have been foulups of some sort when dealing with new telephone prefixes and area codes. In one memorable case, I was trying to straighten out a problem with my mortgage, and the person at the bank never, ever, returned my calls. I was about ready to call in the bank regulators. After leaving quite a few tartly worded messages, I finally managed to get her on the phone, and discovered that every time she called me, she'd gotten an error recording of some sort and had assumed that the number she had was wrong or my phone was out of order. In fact, I had just started

to work at a job with a new PBX with a new set of DID numbers in a new prefix, and the PBX at the bank hadn't heard about my prefix yet. I told her to dial 9-0 and ask the telco operator to place the call in the future.

Even PBXes with class of service restrictions frequently get it wrong. At one place where I consult they forbid international dialing for most lines except for some speed dial codes programmed into the PBX. At least, they think they do. If I dial 011-code-number, I get a fast busy from the PBX. If I dial 01-code-number and make it person to person, it works. If I dial 10288-011-code-number or 10222-011-code number or 10333-code-number, it works. (If only I had some friends in foreign countries to call.)

The local telco has a newsletter that they send out to advise PBX customers of new prefixes, upgrades to CO equipment (which always cause some problems since if nothing else, call progress sounds and the timing of calls change.) There are a lot of changes. As far as I can tell, every PBX that does least cost routing needs to know all of the prefixes in its local area code, and in most cases the updates are typed in by hand using some decidedly user hostile interfaces. If anything, I'm surprised that they get them right as often as they do. In many cases, I suspect that the PBX manager only updates the prefix table when somebody complains.

Telephone calls are routed by what is in effect a tremendous distributed data base that maps numbers to trunks and routes. At least near the fringes, the data base is usually updated by methods that to me at least seem laughably obsolete.

Regards,

John Levine, johnl@esegue.segue.boston.ma.us, {spdcc|ima|lotus}!esegue!johnl

What the SJG Cyberpunk Manual Tells You to Do

J. Eric Townsend <jet@karazm.math.uh.edu> Sat, 2 Jun 90 1:25:34 CDT

Well, I rushed out and bought GURPS Cyberpunk, in the hopes that my money will help SJG with legal fees. (Plus, I collect game stuff.)

On the front cover, in the SJG Illuminatus logo, it says: "The book that was seized by the U.S. Secret Service! (see p. 4)"

Anyway...

(Assuming I know *nothing* about cracking/phreaking. I won't comment on my real knowledge.) The following is a summary of text from the GURPS Cyberpunk supplement, with a few direct quotes.

How Much Hacking Can I Do Based on the C-word manual: (From the section entitled "Netrunning".)

- 0. People use handles to hide their real identity (p62).
- 1. You can uses sensitive devices to listen in on the signals being

sent to a computer monitor, and redisplay the image on your own screen (p62).

2. General info on ISDN. (p64-64)

3. Computer accounts can come in various levels, from specialty logins (uucp) to "superuser" who has access to everything. Some programs can give you a higher level of access, equivalent to a "better" account (p68).

4. General info on back doors (p69).

5. General info on chat systems (p69).

6. A list of network names from around the world. No clues as to which are real. For the US, the following are listed:

WUT, UDTS 2, Datel I & II, Telenet, Tymnet, ARPAnet, Infomaster, GraphNet, TRT, FTCC, UniNet, Autonet, CompuServer, GENIE, AlaskaNet, JANET, Internet (p 71).

7. Passwords can be really obvious, or hard to remember random text strings (p 72.)

8. A program could possibly cause physical damage (p 72.)

9. General Phreaking Info:

- Diverters: go through a bunch of systems so that tracing takes a long time;

- Junction Boxing: Just go down to the local junction box and tie in (p 76).

10. Lots of networks use different protocols that are sometimes incompatible (p 77).

11. Ma Bell stuff:

- Existence of CN/A, and that Ma Bell can look you up in any way;

- Line Routing: "With access to the main phone switch computer,

a hacker can control everything about a specific phone line.";

- Monitoring: a person could monitor calls with the right access;

- After Billing: A person could change bills; (p 82).

12. Trashing: Go through somebody's trash to find out all sorts of interesting info about their computing equipment (p 86,87).(13 and 14 are from the section "Attack and Defense Programs". The programs are obviously s-f software, but...):

13. Promote: "This program is executed from a normal user account on a system. If successful, the account is 'upgraded' to a superuser account."

14. Webster: "This is the standard icebreaker for use against Password programs (see p 93.). It acts as an extremely fast 'brute-force' hacker." (p 92).

15. Credcard Crime: A false balance could be entered in an account.

A device could be used to access somebody else's card without having the correct password to get into the credcard (p 105). [note: a credcard is a self-contained debit card that can have anything from a pasword to retina scan protection.]

And, um, that's about it. Now that you've read that, you know how to break into computer systems and do phone phreaking... 1/2 :-)

J. Eric Townsend -- University of Houston Dept. of Mathematics (713) 749-2120 Internet: jet@uh.edu Bitnet: jet@UHOU Skate UNIX(r)

Re: Word Perfect Software Upgrade Crashes Utah Phone System

Kyle Jones <kjones@talos.pm.com> Sat, 2 Jun 90 17:59:33 EDT

m1wmk00@fed.UUCP writes: > From an Infoworld article on Word Perfect ("Leader of the Pack," > pp. 45-6, May 23, 1990):

>

> "When [Word Perfect] 5.0 shipped in May 1988, the company underestimated

> the demand for telephone support. Although it bought additional phone

> lines, traffic was so heavy that calls to the support department brought

> down the toll-free systems for the state of Utah, including phone systems

> for American Express, Delta Airlines, and the Latter Day Saints Church."

This reminds me of something that happened in my own neck of the woods.

One night I was watching a program on channel 35 when a message flashed on the screen. The message said that the Xth caller would win concert tickets or some such. Since the phone was right beside me, I decided what the hey, and picked up the phone to call. I didn't get a dial tone for the long time. Odd. Finally I heard the tone and dialed the number. I waited. And waited. And waited. No connection, no ringing, no click, nothing.

Thinking I'd misdialed somehow, I depressed the switchhook to try again. I waited for the dial tone. And waited. And waited. And waited! Suddenly it occurred to me, the number began with 358-... my exchange, augh. Apparently the massive influx of calls to the TV station completely hosed whatever gateway there was for my exchange, so I couldn't get a call in edgewise. (Does this sound right to you folks who know something about the phone system?)

Whatever the reason, I'm glad the house wasn't on fire. :-/



Report problems with the web pages to the maintainer



Werner Uhrig <werner@rascal.ics.utexas.edu> Sun, 3 Jun 1990 7:05:39 CDT

[the following is extracted/translated from the Swiss press agency ELSA]

Lausanne, June 2 (sda) Police may not keep any unimportant data captured on a fiche or file for longer than five years on any person. Disrespecting this rule shall be considered contrary to the constitutional right of personal freedom and the right of a person to respect of privacy. This basic ruling was published on Saturday by the Swiss Supreme Court.

[Re: unimportant; don't ask me. no further explanation was given.] [Re: fiche or file; the German words used were "Fiche oder Dossier".

I think that they could better have used an expression like "any form of information storage" - and I assume that using more than one word indicates the intended meaning of "any" rather than limiting the applicability of the law - but naming just these 2 forms of data storage may, no doubt, lead to some lawyer to bicker over this "detail".]

A U.K. View of Early C3 Systems

<F_REYNOLDS@hicom.loughborough.ac.uk> 3-JUN-1990 00:07:04

I have read Les Earnest's contributions on U.S. experience with interest.

In 1970 I found myself employed on Linesman, a massive UK military command and control system. A year later I moved to a nearby university and ended up assessing Master's degree dissertations carried out by "students" working on Linesman.

At the time the project was in deep trouble - in that questions were being asked in Parliament because it was clear that things were going wrong. The basic problem was that there was no comprehension of sunk costs. The cheapest, common sense option of scraping the tons of equipment that had become obsolete before it was ever used was politically unacceptable to the Ministry of Defence. To do this they would have to admit their incompetent management of the project. Perhaps they could escape by throwing even more money to try and buy their way out of the trouble they had got themselves into.

The civilian contractors were paid on a costs plus basis - and the more money the MOD threw at the project the better. In fact they could make even more by cutting back on secretarial staff and getting expensive professional staff to collate the tons of documents the project "required".

Another problem was excessive secrecy - and the "need to know" attitude. For instance, at one time the application design team wanted to know the typical number of Russion bear bombers flying off-shore at any one time. That's too secret to tell you can the reply - until the figure was given on a BBC TV program, having been cleared for public release by a different arm of the Royal Air Force! In fact asking questions was taboo. As a mere minion you did what you were told and no more. I was considered a maverick because I pointed out that the throughput of a particular device would be an order of magnitude less than the design document required. (The design had been based on the maximum hardware timings theoretically possible - and implicitly assumed, for example, that a human could respond to a twin light signal by pressing a heavy duty key in less time than it would take for the filiment in the bulb to cool sufficiently to be visually detectable.) On another occasion I pointed out that programming and systems staff were repeating earlier errors because the results of assessment trials were considered too sensitive to tell them where they had gone wrong. (For this impudence I was was denied an annual increment!)

The effect of the quality of staff was interesting. The salaries paid were above the odds - after all the MOD were desperate and the civilian contractors got a percentage. People being interviewed were not give a fair picture for fear of putting them off. (No one ever though to tell me that I was being interviewed to work on a military project!)

Good staff (and those with a professional concience) quickly realised that they had made a mistake and moved on. This left a residue of unimaginative plodders who couldn't possibly get a better paid job elsewhere, and mecinaries who would do anything for money. This was particularly obvious in their project work at the nearby university, when it was clear that working on the project was teaching them bad obsolete techniques and a belief that staff didn't need to know anything outside their immediate work environment.

But this isn't the end of the affair. When one military project ends the team of out-of-date and inward-looking programmers and systems analysts is not disbanded. Other military projects are out to tender, and the civilian contractor has a ready made team of staff who have security clearance and know how to work to military specifications

Of course my experience is now nearly twenty years out of date - but I still meet people who say that there has been little change.

✓ Glass cockpits (A320, etc.)

<henry@zoo.toronto.edu> Sun, 3 Jun 90 23:58:50 EDT

The April 30 issue of Aviation Week has a couple of interesting small items about computerized airliners and "glass cockpits".

The first is a news item: Airbus Industrie is considering alterations to the A320's flight software to help guard against "overconfidence syndrome", which they consider a significant factor in the Habsheim and Bangalore crashes. One possible change is upgrading the automatic throttle management of the "alpha floor" protection mode to guard against descents with inadequate thrust. "Alpha floor" already runs the throttles up automatically in emergencies like encounters with serious windshear or maneuvers to avoid collisions. Says Bernard Ziegler (Airbus VP Engineering): "The alpha floor was never designed to save a crew that had been improperly managing a normal approach, but we now are thinking of modifying it to serve as one more safeguard. Such a modification will not make it a 100% safeguard, but it could offer an additional safety margin."

The second is a background piece on the poor state of research in glass-cockpit human factors (for example, NASA Ames, a major center of work on such things, has no simulator representative of modern cockpits). Hart A. Langer (United Airlines VP flight operations) says that flight-management-system CRTs act as "cockpit vacuum cleaners -- they suck eyeballs and fingertips right into them. I have given check rides on these aircraft and seen four eyeballs and ten fingertips caught in two [displays] at the same time. This is bad enough at cruise altitude, but it can be lethal in the low-altitude terminal area..."

Henry Spencer at U of Toronto Zoology uunet!attcan!utzoo!henry

Article on A320 in Aeronautique, April 1990

Jon Livesey <livesey@Eng.Sun.COM> Sat, 2 Jun 90 17:11:56 PDT

In <u>Risks-10.02</u> Pete Mellor inadvertently gives us a good example of the risks of muddy thinking.

Writing of a translated article, he recommends it to us on several ground, one of which is

> b) the fact that it presents a French (and therefore not negatively biased?)> view,

The two problems with this are, first, Airbus is not exclusively a French aeroplane. It is a joint venture between several European countries.

Secondly, there has been quite a lot of negative comment about Airbus from French sources, mainly from pilots' unions.

The risk here is that of giving one source extra credence on specious grounds.

Moeing 747-400 Autothrottle problems

Martyn Thomas <mct@praxis.UUCP> Wed, 11 Apr 90 17:26:41 BST

This week's Flight International reports:

"British Airways (BA) Boeing 747-400s have experienced uncommanded inflight closure of all four throttles on six separate flights between 6 October 1989 and 19 February 1990, 'several times' on one of those flights alone, according to formal reports. Several other airlines have suffered the same incident, Northwest reporting it first. ...

In most of the events the power levers retarded rapidly to idle, but sometimes the reduction was partial, followed by automatic reset. ...

All incidents have occurred in the climb or cruise, and an IAS of more than 280 Knots is believed to be fundamental to the event. ...

Evidence indicates that the event is caused by a spurious signal to the full authority digital engine control from the stall-management module. The 'single-word' spurious command says that the undercarriage [gear] is down or the flaps are at setting 1, so if the IAS exceeds the maximum speed for these configurations, the autothrottles close to reduce IAS to limiting speed, then

reset to maintain it.

The modification [to correct the problem - issued on February 22nd] assumes that the fault was in the processing logic of the appropriate universal logic card (a printed-circuit software unit [sic]) and adopts a standard technique for reducing digital oversensitivity: there is now a delay (a few miroseconds) built into the software by requiring it to receive an 'eight-word' command before acting. Power spikes of other spurious commands should not produce a reaction.

So far the latest modification has proved effective. Early corrections, though, had assumed the reaction was associated only with main-gear selection, so although software changes had reduced the incident rate, spurious flap signals continued to set engines to idle. BA has not reported any further events since February."

[end of quote]

This looks like a useful warning of inability to get complex systems right luckily it only occured at high IAS and was sub-critical for flight safety. I hope that appropriate lessons are learnt by both developers and certification authorities, and that they start to question their ability to assure the safety of such systems.

Notice that the partial fix, reported in the last paragraph, implies that the Flight Data Recorder either was not used to diagnose the fault, or contained insufficient information to point the finger at both the gear and flap signals. This seems ominous for future accident cause analysis. The apparent action of fixing symptoms until no further errors are reported, rather than analysing the cause and then looking for all possible classes of the same error, seems ill-judged, too.

I wonder what re-certification was undertaken following the modification.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

✓ Equipment failure or human failure? (<u>RISKS-10.01</u>)

<ark@research.att.com> Sun, 3 Jun 90 00:12:55 EDT

Henry Spencer wonders if the failure of the pilot who had problems with the `glass cockpit' to come forth means that something more was going on than meets the eye.

It's possible, of course, but if the UK Civil Aviation Authority is anything like the FAA, I'm not surprised the pilot is keeping quiet. It's rather amazing how nasty the FAA can be if it decides to go after someone. ...

Æquipment failure or human failure? (<u>RISKS-10.01</u>)

<julian@riacs.edu> Sun, 03 Jun 90 22:57:01 -0700

>Some little while ago, Risks published the report of a flight crew landing an >airliner in Britain after a very difficult time with wind readings of 100+

>problem are hamstrung, doubts are cast on the accuracy of the report, and if it >*is* factual, that aircraft is still in service and potentially a lethal hazard >to crews and passengers.

They aren't the only ones. Here is an excerpt from "Tales from the TRACON: a controller's view of emergencies" in June 1990 "IFR" 6(6). Belvoir Publications, 75 Holly Hill Lane, Greenwich, CT 06836 (all typos mine):

It's frequently the same for controllers. We're sometimes reluctant to take any action that invites scrutiny of our routine work. An experience I had last year shows what can happen. During one shift on a typical hectic IFR day in the TRACON, my frequency died three times. Technicians reviewed the problem, only to find the "bad" frequency had started working again. After three such outages (with no repairs) I filed an unsatisfactory condition report (UCR) which goes straight to Washington and requires an answer to the complaint in writing. Not surprisingly, facility managers aren't too fond of UCRs.

When my complaint was checked out, my tapes were "dumped" (supposedly to discover whether the outage reqallly happened) on *every* position and frequency I had worked that day, not just the "bad" frequency. The tapes showed that I had really had a problem. But in the process, management had my supervisor "counsel" me for bad phraseology and improper land line usage. The experience hardly encourages one to draw attention to malfunctions or emergencies.

A few days ago I posted to rec.aviation a white paper by an ARTCC controller detailing how certain kinds of targets could be eliminated from the controller's scope by the computer, roughly because it didn't like the targets. Washington's response to his UCR was that they didn't see a problem.

Dr. Julian Gomez RIACS - Research Institute for Advanced Computer Science

Ke: Steve Jackson Games (Webb, <u>RISKS-10.01</u>)

Jim Harkins <jharkins@sagpd1.UUCP> 2 Jun 90 22:01:48 GMT

>The chance of GURPS Cyperpunk being used as a manual for computer crime is very >slight indeed. I don't see where this is relevant. Its perfectly legal to buy books on how to make illegal stuff like explosives, check out the warnings section(s) in college chemistry books, not to mention stuff like The Poor Mans James Bond. There are some very good cookbooks on committing murder (see the mystery section of Waldenbooks). Should we have thrown Agatha Christi in the slammer? So what would make it illegal to give even a step by step list of instructions for breaking into a computer?

It seems to me that the act of commiting a crime is illegal, but the knowledge of how to commit that crime isn't. I think we can all figure out on our own how to stick a gun into a cashiers face to get money, but we haven't done anything wrong until we actually do it. Nor have I done anything wrong by offering a suggestion on improving your monthly income :-) Of course, if I suspect that you did use my suggestion then by not finking on you I am breaking the law.

jim

routing tables for private switches

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Sat, 2 Jun 90 11:47:00 EDT

It is a general problem that NYNEX has not been automatically distributing routing updates to people who own their own switches. This is one of the things that NYNEX does to discourage companies from owning their own switches and encourage them to use Centrex.

If you think that this is bad public policy, call the public utility comission's complaint number.

Risks of Caller Identification

David Lesher <wb8foz@mthvax.cs.miami.edu> Sun, 3 Jun 90 18:16:14 EDT

The law enforcment community in FL is upset over Bell South's plan to offer Caller ID without subscriber blocking. While the telco has offered blocking to law enforcement officers, and a few select others, they are still worried because:

1. The utility will need to have a list of all those eligible, including undercover officers.

2. The fact the CID is blocked is a sure pointer that the caller is a cop, sure death to an informant.

I soon thought of a third. The blocking is done in the terminating CO. What happens if the expected block fails, for whatever reason? There is no feedback to the caller that such has happened.

Given the level of violence within the general population around here, the CID

block seems to made a classic RISKS mistake. A system designed for less critical use has been thrust beyond its design parameters into a life-dependent role. This strikes me as no different than using unproven software for designing bridges or buildings.

More sendmail woes (duplicates of <u>RISKS-10.02</u> for a few of you)

Peter G. Neumann <neumann@csl.sri.com> Mon, 4 Jun 1990 9:32:45 PDT

HERCULES crashed at 6AM this morning, but the completion of the mailing of RISKS-10.02 had been hung in the queueueueueueuemanager since Saturday for just one of the six RISKS sublists --so a few of you got a second copy of RISKS-10.02 when the system automatically rebooted. This is of course Standard Sendmail Problem Number 1. (Unfortunately the log tapes do not explain the crash!) This problem reinforces the need for a more robust algorithm that more often deletes nonNACKed sendings periodically from the queue during the first pass over the long list, rather than waiting (hopefully) for the end of the list. Private hacks of sendmail exist to do that, but each privately hacked version of sendmail seems to introduce its own set of new problems or else does not provide the services of other hacked versions. At any rate, mailing to very large lists remains a tricky business.

Ironically, I had just prepared a bunch of slides for the talk on my COMPASS paper at the end of the month, The Risk of the Year: Distributed Control, which (among other things) relates the 15 Jan 90 AT&T problem to the 1980 ARPANET collapse, and throws in a section on sendmail woes for good measure.



Search RISKS using swish-e

Report problems with the web pages to the maintainer

Volume 9 Issue 5 (15 Jul 89)

- UK Defence Software Standard (Dave Parnas, Nancy Leveson, Dave Parnas)
- DARPA contract: use AI to select targets during nuclear war (Jon Jacky)
- "Flying the Electric Skies" (Steve Philipson)
- Automobile Electronic Performance management (Pete Lucas)
- Volume 9 Issue 6 (18 Jul 89)
 - Mitnick sentenced as an addict (Rodney Hoffman)
 - Long addresses confuse bank's computer (Paul Leyland)
 - Town Hall's computer snags trouble old age pensioners (Olivier Crepin-Leblond)
 - <u>Re: Automobile Electronic Performance Management (Charles Rader)</u>
 - Re: UK Defence Software Standard, non-determinism, recursion and armageddon (Victor Yodaiken, anonymous via Tim Shimeall, Bob Estell, Martin Minow)
 - Telephone technicians tapping into other phone lines (Olivier Crepin-Leblond)
 - Re: New Yorker Article on "radiation" risks (Gordon Hester)
- Volume 9 Issue 7 (19 Jul 89)
 - Re: Gordon Hester on Paul Brodeur (Radiation) (Jan Wolitzky)
 - <u>Computers consume wine (Hugh Davies)</u>
 - Mitnick sentence (Rodney Hoffman)
 - Re: DARPA contract: use AI to select targets during nuclear war (Lee Naish)
 - <u>Reliance on technology (Jake Livni)</u>
 - Summer slowdown for RISKS (PGN)
- Volume 9 Issue 8 (28 Jul 89)
 - Returning before departing on airline reservation systems (Gary McClelland)
 - Sun security problem: restore (J. Paul Holbrook)
 - <u>Computer condom? (Jeff Stout)</u>
 - <u>Robert Tappan Morris indicted (Steve Den Beste)</u>
 - <u>Re: UK Defence Software Standard (Mark Moraes, Douglas W. Jones)</u>
 - Polling vs. interrupts (Douglas W. Jones)
 - Software Engineering Models (John (J.G.) Mainwaring)
 - Single Point of Failure for Internet Management (Kee Hinckley)
 - DARPA contract & AI for moving targets (Bob Estell)
 - Two-Word Last Names and Other Amusing Database Stories (Gary McClelland)
 - Credit card issuers invade cardholders' privacy (Andrew Klossner)
 - <u>Re: windowless cockpits (Andrew Klossner)</u>
- Volume 9 Issue 9 (14 Aug 89)
 - California to escrow electronic vote counting software (Rodney Hoffman)
 - <u>Voters Left off Electoral Roll (Rohan Allan Baxter)</u>
 - Beeperless remote answering machine risks (Peter Scott)
 - <u>Computerized Houses (Jake Livni)</u>
 - Automated Driving (lan Gent)
 - Marijuana Virus wreaks havoc in Australian Defence Department (J. Holley)
 - Universal Trapdoors (Vin McLellan)
 - <u>Computer Problems at Saratoga Racetrack (Rodney Hoffman, Dave Fiske)</u>
 - RISKS summer reruns? (Daniel F. Fisher, Jim Horning)
- Volume 9 Issue 10 (14 Aug 89)
 - KAL007 jury finds "willful misconduct" (Clifford Johnson)

- California studies "drive-by-wire" (Rodney Hoffman)
- NY State DMV Computer RISKS (Will Martin)
- <u>RISKS is back in gear (almost) (PGN)</u>
- "Radiation" or "Fields" (Jerry Leichter, Irving Wolfe, John H. Martin, Irving L. Chidsey, Klaus Rieckhoff)

Volume 9 Issue 11 (15 Aug 89)

- Cellular Telephone Causes Airliner Fire Alarm (Dave Davis)
- Computer-based airline ticket scam (Rodney Hoffman)
- New Yorker Article on EMF Risks (Gordon Hester, Dan Schlitt)
- 1989 CPSR Annual Meeting (Gary Chapman)

Volume 9 Issue 12 (17 Aug 89)

- RISKS IS FINALLY MOVING TO CSL.SRI.COM! (PGN)
- Flaws in calculations, computer models in Trident failures (Jon Jacky)
- Voyager 2 software faults at launch, 1977 Aug 20 10:29 (David B. Benson)

Volume 9 Issue 13 (18 Aug 89)

- Phony IRS refunds by computer (Rob Gross)
- Cellular phones in stings (David Wittenberg)
- <u>Aircrew acceptance of flight automation (Robert Dorsett)</u>
- Unauthorized Internet activity (CERT Internet Advisory -- Kenneth R. van Wyk)
- Re: Marijuana virus wreaks havoc in Australian Defence Department (Anthony John Apted)
- More on the Wily Hackers (Rob Gross)
- Training and Software Engineers (Tim Shimeall)
- Computer-based airline ticket scam (Jordan Brown)

Volume 9 Issue 14 (21 Aug 1989)

- The Check's in the Mail (but the water got shut off anyway) (Dave Clayton)
- Australian Commonwealth Bank -- doubled deposits (Martyn Thomas)
- Automatic vehicle navigation systems (Pete Lucas)
- Tired of computers being trusted? (a balancing act for wheel watchers) (PGN)
- Re: Computer-based airline ticket scam (Jules d'Entremont)
- Human failures in emergencies (Henry Spencer)
- Hazards of Airliner Computerization (Mike Trout)
- Re: California studies "drive-by-wire" (John Chew)
- First test for electronic tagging starts in jail! (Olivier Crepin-Leblond)
- Re: unauthorized Internet activity (anonymous)
- DEMO Software Disk Infected (Jerusalem Version B) (J. Vavrina)

Volume 9 Issue 15 (22 Aug 1989)

- Toronto Stock Exchange down for 3 hours, disk failures (Peter Roosen-Runge)
- Automated highways ... (Jerry Leichter, Bill Gorman, Peter Jones, Emily H. Lonsford, Bill Murray)
- <u>Constructive criticism? Technology doesn't have to be bad (Don Norman)</u>
- Computer Ethics (Perry Morrison)

Volume 9 Issue 16 (23 Aug 1989)

- Autopilots (Marc Rotenberg)
- Hazards of Airliner Computerization (Brinton Cooper)
- Risks, and an assumed definition of "reliability" (Bob Estell)
- Computers in Medicine (Brinton Cooper)
- Constructive criticism? Technology doesn't have to be bad (Donald A Norman)

- Tandem computers and stock exchange failure (Ernest H. Robl)
- TSE shutdown -- a success story (Rich D'Ippolito)
- Incompatible IR controllers damage circuits? (David A Willcox)
- Re: a balancing act for wheel watchers (J. Eric Townsend, Keith D Gregory)

Volume 9 Issue 17 (23 Aug 1989)

- Hazards in Airliners and Medicine (Nancy Leveson)
- <u>Re: Technology Doesn't Have to Be Bad (Mike Trout, Robert Dorsett)</u>
- "Drive-by-wire": What about bicycles? (Anne Paulson, Donald A Norman)
- <u>Re: Autopilots (Brinton Cooper)</u>
- <u>Re: Automated Highways (George H. Feil)</u>
- Roads made safer or not? (Pete Lucas)
- Training & Software Engineering, a reply... (Edward A. Ranzenbach)

Volume 9 Issue 18 (28 Aug 1989)

- Proposal for SDI software center (Gary Chapman)
- Computerworld article on high-tech weapons (George Entenman)
- CHAOSNet used in `SNUFF' snuff (PGN)
- DMV records, and individual privacy and safety (PGN)
- Another vehicle guidance system (Pete Lucas)
- <u>Medics touch computers?!? (Sam Bassett)</u>
- Unfounded fault-probability claims (Dieter Muller)
- Lowest-bidder or weak specs? (David A Honig)
- Automated roads, drive-by-wire, bicycles, and the elderly (PGN)
- The Guardian vs computer passwords (Brian Foster)
- Volume 9 Issue 19 (30 Aug 1989)
 - NEW INSTRUCTIONS TO FTP VOL i ISSUE j, effective immediately (PGN)
 - Reg. of Motor Vehicles computer slows down (Adam Gaffin)
 - British nuclear reactor software safety disputed (Jon Jacky)
 - South German hackers hack TV German Post (Klaus Brunnstein)
 - Ethics (Donald J. Weinshank via Tom Thomson)
 - sci.aeronautics, a new newsgroup (Robert Dorsett)
 - What's a stamp? (postal service problems) (David Elliott)
- Volume 9 Issue 20 (1 Sep 1989)
 - Last Night's "Tonight" was Unknighted; Cars on Carson Top Hat Trick (PGN)
 - More on the Therac 25 -- by Jon Jacky (PGN)
 - Witness questions attack on Iranian jet (Robert Dorsett)
 - <u>Risks of on-line course registration (Deborah M. Clawson)</u>
 - <u>Specifications (Martyn Thomas)</u>
 - Re: Lowest-bidder or weak specs? (Scott, Robert Hirsch, Bill Cattey)
 - Pilot simulator training and boredom (Dan Franklin)
 - More on automation (Robert Dorsett)
- Volume 9 Issue 21 (5 Sep 1989)
 - <u>Re: Technology doesn't have to be bad (Brian Randell)</u>
 - Medical systems and RF interference (Edward A. Ranzenbach)
 - <u>`Business Week' on computers and privacy (Rodney Hoffman)</u>
 - Law == Ethical Consensus (Scott Guthery)
 - US occupational hazards much worse than in Europe, report claims (Jon Jacky)

Are on-line pictures RISKy? (Russ Nelson)

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

Volume 9 Issue 22 (6 Sep 1989)

- Paris computer takes law into its own hands (ST4012704 and Sally Jubb)
- Brian Randell's comment on fault/failure analysis (Ted Lee)
- Re: US occupational hazards much worse than in Europe (Mats Ohrman)
- Re: medical systems and RF interference (Brian Kantor)
- Re: mis-tagging (Olivier Crepin-Leblond)
- Electronic House Arrest Failure (Martyn Thomas)
- Re: Lowest-bidder or weak specs? (Henry Spencer)
- <u>Re: Law == Ethical Consensus (Douglas W. Jones, Victor Yodaiken, Gilbert Harman, Eric Hughes, Bill Murray,</u> Joel M. Halpern)
- Volume 9 Issue 23 (12 Sep 1989)
 - <u>Risks of RISKS: A bug in sendmail and multiple copies of RISKS-9.22</u> (PGN, with help from Bill Sommerfeld and Jeff Schiller)
 - RF susceptibility of electronics (Pete Lucas)
 - Some background on the French Farce (Dave Horsfall)
 - Organizational Accreditation for Computer Assurance: Some Ideas (Frank Houston)

Volume 9 Issue 24 (14 Sep 1989)

- RISKS-9.22 and RISKS-9.23 problems had different causes! (PGN)
- Risks of RISKS: A bug in sendmail and RISKS-9.22 (Scott Mueller)
- Phobos 1 & 2 computer failures (Ralph Hartley)
- Aircraft simulators (Rob Boudrie)
- Speeders' Delight? (Anthony Stone)
- Medical accreditation: based on "customer" clout? (Bob Ayers)
- RISKS in mainstream entertainment (Mission Impossible) (Benjamin Ellsworth)
- Software Safety Standards (Anthony J Zawilski)
- 12th National Computer Security Conference (Jack Holleran)
- Volume 9 Issue 25 (15 Sep 1989)
 - Risks of distributed systems (Eugene Miya)
 - Medical accreditation: good for big shops only? (Douglas W. Jones)
 - The role of government regulation (Douglas W. Jones)
 - Is modern software design contributing to societal stupidity? (Tom Comeau)
 - Re: Aircraft simulators (Alan J Rosenthal, Robert Dorsett)
 - Mission: Impossible (Robert Dorsett)
- Volume 9 Issue 26 (20 Sep 1989)
 - Hospital problems due to software bug (Joe Morris)
 - Man-Machine Failure at 1989 World Rowing Championships (Geoffrey Knauth)
 - Responsibility, Doctors, Military vs Software Developers (Leslie DeGroff)
 - Organizational Accreditation: More Thoughts (Frank Houston, Jon Jacky)
 - An interesting answer to the distributed time problem (Roy Smith)
 - Re: Risks of distributed systems (D. Pardo)
- Volume 9 Issue 27 (21 Sep 1989)

- Re: Brian Randell's commentary on safety analysis (Nancy Leveson)
- Re: Risks of Distributed Systems (Charles Shub)
- Re: Hospital problems due to software bug (Will Martin)
- Mailer Bug moves to MCI? (Jerry Durand)
- Loose wires, master clocks and satellites (Peter Jones, PGN)
- Volume 9 Issue 28 (24 Sep 1989)
 - USAir 737-400 crash at LaGuardia (PGN)
 - Re: Hospital problems due to software bug (Steve VanDevender + Amos Shapir)
 - Computers, Planning, and Common Sense (John (J.G.) Mainwaring)
 - Synchronizing Clocks (Earl Boebert)
 - <u>Re: Risks of Distributed Systems (Sung Kwon Chung)</u>
 - Master clocks, etc. (Eddie Caplan)
 - ISO 9001 accreditation (Martyn Thomas)
 - Toxic Spill at the Department of Education [long] (Joe Pujals)
- Volume 9 Issue 29 (25 Sep 1989)
 - Computerized fingerprint system has human failure (Dave Suess)
 - Computerized translation strikes again (Joe Morris)
 - Loose wires (Desmond Andigo via John Leonard)
 - Software *IS* an abstraction (Bob Estell)
 - Yes, the power grid IS getting less reliable (Bruce Hamilton)
 - Computers, Planning, and Common Sense (Richard O'Keefe)
 - Simulated aircraft emergencies (John Mackin)
 - Re: Software Accreditation (Richard Threadgill)

Volume 9 Issue 30 (2 Oct 1989)

- The Cuckoo's Egg (Cliff Stoll)
- Internet cracker on the loose (Barry Lustig)
- Late night system administration == trouble on SunOS 4.x (Angela Marie Thomas)
- Date manipulation and end of millennia (Pete Lucas)
- Re: An interesting answer to the distributed time problem (Randall Davis)
- Re: Man-Machine Failure at 1989 World Rowing Championships (Randall Davis)
- Volume 9 Issue 31 (4 Oct 1989)
 - Computer multiplies taxable earnings by 100 (Rodney Hoffman)
 - Hackwatch spokesman charged (Dave Horsfall)
 - Re: Internet cracker on the loose (Randy Buckland)
 - Re: Hospital problems due to software bug (Mike Kimura)
 - Re: Date manipulation and end of millennia (Henry Spencer)
 - Re: Clock-watching (George L Sicherman)
 - 9-digit precision (Gideon Yuvall)
 - The Risks of Crossing the Tracks (Railroad Crossing Gate Technology) (Jean- David Beyer, Laurence Larry Sheldon, Richard L. Piazza via Chuck Weinstock).
 - Fifth Annual Computer Security Applications Conference (Marshall D. Abrams)
- Volume 9 Issue 32 (16 Oct 1989)
 - Missed zero blamed for aircrash (Dave Horsfall)
 - Software reliance/software problems and the Stealth (Marc Rotenberg)
 - Coping with the unexpected Friday's stock plunge (Steve Bellovin)
 - Re: latest stock market crash (Olivier Crepin-Leblond)

Atlantis launch delay (PGN)

- Keeping up with the [Indian(a)] Joneses in elections (PGN)
- Friendly advice... [Datacrime] (David Gursky)
- Re: Synchronizing Clocks (Brian Randell)
- Volume 9 Issue 33 (22 Oct 1989)
 - Earthquake preparedness in computing (PGN)
 - <u>Air-Traffic Disruptions (PGN and Robert Dorsett)</u>
 - <u>Railroad Level-Crossing Monitoring (Brian Randell)</u>
 - Sometimes touch-screens aren't user-friendly (Jeffrey Mogul)
 - UK Banking Error (Brian Randell)
 - Quotron gores the bears and bares the bulls (PGN)
 - Quotron software timing error (David B. Benson)
 - Re: latest stock market crash (David Gursky)
- Volume 9 Issue 34 (24 Oct 1989)
 - Earthquake and Computers (Bill Murray)
 - Black Friday was only grey in Boston (Pete Kaiser)
 - Human chess supremacy at risk? (Bob Barger)
 - <u>CERT Ultrix 3.0 Advisory (Ed DeHart)</u>
 - CERT DECnet Worm Advisory (Ed DeHart)
- Volume 9 Issue 35 (25 Oct 1989)
 - Offensive message on electronic information board (Bob Morris, John Crider)
 - 14-year-old cracks TRW credit for major fraud (Rodney Hoffman)
 - Foreplay Doesn't Effect Response Time (Don Hopkins)
 - "Computer Virus Countermeasures" Article (Will Martin)
 - Hardware failure mimics hackers (Rob Wright)
- Volume 9 Issue 36 (27 Oct 1989)
 - Bug in Intel 486 chip (PGN)
 - UK Banking Error (Brian Randell)
 - The Presentation of Risky Information (Joshua Levy)
 - Hardware failure mimics hackers (Pat White, Andy Goldstein)
 - Worms in a data stream (Rick Simkin)
 - CERT Advisory on Sun RCP (J. Paul Holbrook)
 - Warning About CERT Warnings (anonymous)
 - Licensed users exceeded (Tim Steele)
 - A lesson involving 'CRACKERS' (APPLE II) (Olivier Crepin-Leblond)
- Volume 9 Issue 37 (29 Oct 1989)
 - Low-tech wins the day in airliner mishap (Glenn Story)
 - Hi-tech loses in cars (Alayne McGregor)
 - Re: Hardware failure mimics hackers (Sukumar Rathnam)
 - Re: Black Friday in Boston and manual systems (D. W. James)
 - Re: Human chess supremacy at risk? (Andrew Klossner)
- Volume 9 Issue 38 (31 Oct 1989)
 - Passwords in the Electronic Home (Gary McClelland)
 - A new excuse (Ernest H. Robl)
 - Hot computers and temperature-sensitive programs (Donald Arseneau)

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

Volume 9 Issue 39 (7 Nov 1989)

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

Volume 9 Issue 40 (10 Nov 1989)

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

Volume 9 Issue 41 (11 Nov 1989)

- Stuffing the electronic ballot box (again) (PGN)
- BART and the Bartered-Computer Commuters
- Coral reef ruined by poor user interface design? (Jim Helman)
- Re: Computer errors and computer risks (Jerome H Saltzer)
- <u>Computer used to find scoflaws in Boston (David desJardins)</u>
- Reference on the early history of Ada -- killing reliably (Eugene Miya)
- Volume 9 Issue 42 (13 Nov 1989)
 - Equinox TV programme on A320 (Bev Littlewood, Chris Dalton)
 - European Safety is not always BETTER (Bruce C. Brown)
 - <u>Artificial lightning (PGN)</u>
 - Another intrusive database with associated privacy problems (Bill Gorman)
 - Re: "Computer Error" in Durham N.C. election results (Gregory G. Woodbury)
 - <u>Re: Computer errors and computer risks (Willis H. Ware, D. King)</u>

Volume 9 Issue 43 (15 Nov 1989)

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

Are you sure you declared ALL your dividends? (Peter Jones)

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

Volume 9 Issue 44 (17 Nov 1989)

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

Volume 9 Issue 45 (20 Nov 1989)

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

Volume 9 Issue 46 (22 Nov 1989)

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

Volume 9 Issue 47 (24 Nov 1989)

- Air Force Radar Risk (update) (Henry Cox)
- Congressional report: "Bugs in the Program" (Gary Chapman, Dave Davis)
- <u>Re: Specifying vs. defining (Dave Platt)</u>
- Training programmers (Lee S. Ridgway)
- Re: Privacy and risks in credit information (John DeBert)
- Re: Automated Bank RISKS (Marc Shannon, Jon Mauney)
- <u>Re: Autodialing horror stories (Robert Sansom)</u>
- Volume 9 Issue 48 (25 Nov 1989)
 - Check inquiry / binary search (anonymous)
 - Re: Training programmers (Paul J. Mech)
 - <u>Telephone Overload (Jon von Zelowitz)</u>
 - Write protect tabs (via Peter Jones from Craig Finseth in VIRUS-L)
 - High error rates (P.E.Smee)
 - Policy vs. the Enabling Technology (Bill Murray)
 - Computer Virus Catalog Index: November' 89 (Klaus Brunnstein)
 - CERT_Tools_Announcement (Edward DeHart)

Volume 9 Issue 49 (27 Nov 1989)

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

Volume 9 Issue 50 (3 Dec 1989)

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

Volume 9 Issue 51 (5 Dec 1989)

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

Volume 9 Issue 52 (8 Dec 1989)

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

Volume 9 Issue 53 (11 Dec 1989)

- Computerized public records boon to private eyes probing suitors (Jay Elinsky, Jon von Zelowitz)
- Should computers be legally responsible? (A. Lester Buck)
- <u>Automatic toll systems (Jerry Harper)</u>
- <u>Software Development (Bill Murray)</u>
- <u>Newsgroup posting rejected, rejected, rejected, ... (Earle Ake)</u>
- <u>Comments on Unix INDENT program (Simson L. Garfinkel, Nick Lai, David McAllister)</u>
- Volume 9 Issue 54 (12 Dec 1989)
 - Mariner I [once more] (Mark Brader and Fred Webb)
 - Re: Software tool (indent) munges code (Mark Moraes [2x], Joe Dellinger, Amos Shapir)

- Re: SSA software maintenance (Dan Franklin)
- Re: Don't Give Social Security Numbers to Girlfriends (Will Martin)
- Volume 9 Issue 55 (18 Dec 1989)
 - Risks of Mail (the "yellow peril"?) (Joe Dellinger)
 - PR RISKs of computer communications -- Prodigy (Mark Jackson)
 - Re: private eyes probing suitors -- Amazon Women on the Moon (Dwight McKay)
 - Faults in 29000 RISC chip (Jon Jacky)
 - The Trojan horse named "AIDS" (contributed by many who are not neigh-sayers)
- Volume 9 Issue 56 (21 Dec 1989)
 - GAO Says IS technology is transforming the Government (Dave Davis)
 - California Supreme Court endorses computerized horoscopes (Clifford Johnson)
 - Software malpractice (Steve Philipson)
 - Computerized card catalog (Roy Smith)
 - Frustrated with phones (Shamus McBride)
 - 23 years MTBF ??? (David A. Honig)
 - Re: Another runaway military computing project: WWMCCS (Tom Reid)
 - Virus Hearing on TV (Marc Rotenberg)
 - <u>Risks of posting to risks!</u> (Joe Dellinger)

Volume 9 Issue 57 (4 Jan 1990)

- Self-Service ordering in retail establishments (Russell McFatter)
- Programming Languages and Romanian Dictators (Eric Haines)
- <u>`Credit Card' found from 13th Century (Steve Crocker)</u>
- <u>Risks of computerfax (Steve Elias)</u>
- Password Security: A Case History, by Bob Morris and Ken Thompson (PGN)
- "What Really Happened Oct. 13" (Joe Morris)
- The risks of not learning? (Al Arsenault)
- RAND has not received "AIDS Information Disk" (Correction from Jim Gillogly)
- Call for Papers -- 13th National Computer Security Conference (Jack Holleran)
- Volume 9 Issue 58 (9 Jan 1990)
 - New-Years' Lotto goes Blotto (Jim Anderson)
 - <u>Railroad interlocking systems (Douglas W. Jones)</u>
 - Sorry, the bank's already debited your mortgage (Dave Horsfall)
 - Positive fingerprint identification? (Dave Horsfall)
 - Re: Password Security: A Case History (Fernando J. Corbato)
 - The risks of not learning and of ignoring realities (Jerry Leichter)
 - 6th Chaos Communication Congress, Hamburg 27-29 Dec 1989 (Klaus Brunnstein)
- Volume 9 Issue 59 (10 January 1990)
 - Drawbridge opens without warning in rush-hour traffic (Jon Jacky)
 - Massive Electrical Failure in a Bus (Peter Jones)
 - What hung the computer? (Julian)
 - Passwords and security (Phil Ritzenthaler, Henry Spencer, Jerry Leichter, ark, Peter da Silva)
 - IEEE Symposium on Research in Security and Privacy, Oakland 1990 ()
- Volume 9 Issue 60 (15 Jan 1990)
 - The C3 legacy: top-down goes belly-up recursively (Les Earnest)
 - Dispatchinate Computerized Cab Service (PGN)

- <u>Risks of manual page formatters and inserted text (J. Eric Townsend)</u>
- <u>Re: What hung the computer? (Dave Platt)</u>
- Perils of not planning for errors (Ted Shapin)
- Wrong 800 numbers (Steven W. Grabhorn)
- Password Sharing (Dave Bafumo)
- Call for papers for computer security foundations workshop (John McLean)
- Volume 9 Issue 61 (20 Jan 1990)
 - Shortage of RISKS but no shortage of risks -- the week in review (PGN)
 - AT&T Failure (Bill Murray, Jim Horning)
 - Risks of Voicemail systems that expect a human at the other end (R. Aminzade)
 - <u>Risks of vote counting (Alayne McGregor)</u>
 - <u>Risks of supermarket checkout scanners (David Marks)</u>
 - European R&D in Road Transportation (Brian Randell)
 - Old habits die hard (Dave Horsfall)
- Volume 9 Issue 62 (26 Jan 1990)
 - Australian medical database linkages (Michael Bednarek)
 - Cause of AT&T network failure ("Telephony", Jim Harkins)
 - London Stock Market Disruption (courtesy of Steve Milunovic)
 - Railway interlocking (Clive Feather)
 - More risks to computers (Richard Thomsen)
 - Re: Risks of supermarket checkout scanners (Marvin Moskowitz, Doug Renner, Don Craig)
 - Robert T. Morris Convicted (Michael J. Chinni)
 - <u>Advance Program for Oakland Symposium (REVISED) (Debbie Cooper)</u>
- Volume 9 Issue 63 (31 Jan 1990)
 - Vive la difference? (Peter G. Neumann)
 - Airbus crash of June 88 (Olivier Crepin-Leblond)
 - AT&T Crash Statement: The Official Report (Don H Kemp via Geoff Goodfellow)
 - Important Lesson from AT&T Tragedy (Bill Murray)
 - Potential Lesson From AT&T (Bill Murray)
 - Sun Sendmail Vulnerability (Kenneth R. van Wyk)
 - GPO Library disk infection (PC) (Kenneth R. van Wyk)
 - Re: Password Sharing (Al Arsenault)
 - Annual Computer Security Applications Conference (Marshall D. Abrams)
 - Virology (Gene Spafford)

Volume 9 Issue 64 (1 Feb 1990)

- SENDMAIL horrors (PGN)
- Software error at Bruce nuclear station (Mark Bartelt)
- <u>New South Wales Police deregisters police cars (Diomidis Spinellis)</u>
- Fire and 753 controllers (need a light?) (Neal Immega via Mark Seiden)
- The substantiative error made by AT&T (Robert Ullmann)
- <u>Re: AT&T Crash Statement: The Official Report (Bob Munck)</u>
- Re: Airbus crash of June 88 (Robert Dorsett)
- Re: Virology and an infectious date syndrome (Gene Spafford)
- Volume 9 Issue 65 (2 Feb 1990)
 - The C3 legacy, Part 2: a SAGE beginning (Les Earnest)
 - Sendmail Flaw (Geoffrey H. Cooper)
Filing 1040 Electronically (Bill Murray)

- Predicting Problems (David desJardins)
- Airbus crash (Dave Morton)
- The Trojan horse named `AIDS' revisited (PGN)
- Volume 9 Issue 66 (5 Feb 1990)
 - Another SAGE memoir (Jon Jacky)
 - DoD plans another attack on the "software crisis" (Jon Jacky)
 - <u>The Cultural Dimensions of Educational Computing (Phil Agre)</u>
 - Vincennes' Aegis System: Why did RISKS ignore specifications? (R. Horn)
 - <u>Computer Virus Book of Records (Simson L. Garfinkel)</u>
 - Re: AT&T (Gene Spafford, David Keppel, Stanley Chow)
 - Sendmail (Brian Kantor, Rayan Zachariassen, Geoffrey H. Cooper, Kyle Jones, Craig Everhart).
 - <u>Re: Risks of Voicemail systems (Randall Davis)</u>
- Volume 9 Issue 67 (8 Feb 1990)
 - Shoplifting and Computers (Curtis P. Yeske)
 - New movie Script writer (Olivier Crepin-Leblond)
 - Re: Computers, good and evil (George L Sicherman)
 - The C3 legacy, Part 3: Command-control catches on (Les Earnest)
 - Vincennes' ROEs revisited (Clifford Johnson)
 - SOGS Hubble Space Telescope software now ready (Rodney Hoffman)
 - AT&T and reentrant code (John A. Pershing Jr)
 - AT&T and error recovery (Jonathan I. Kamens)
 - Dillard's Dept Stores Use SSN as Sales ID Printed on Receipts (Allen Gwinn)
 - AutoAlarms (Robert J Woodhead)
- Volume 9 Issue 68 (14 Feb 1990)
 - Re: Caller ID (NYTimes editorial) (John M. Sullivan)
 - How to make answering machines deliver ransom messages (Denis Coskun)
 - More on the Hubble Space Telescope (Hank Strub)
 - Human blamed, not the computer! -- jury duty (Lee S. Ridgway)
 - Accents are more than just decorations (Kai-Mikael J{{-Aro}
 - [Parse-ly, Rosemary, Time, Light, Control & Other SAGE Remarks] (Martin Minow)
 - Blazers (Jeff Berkowitz)
 - Re: Computers, good and evil (Gregg TeHennepe)
 - <u>Telephone Switch Security (Roland Ouellette)</u>
- Volume 9 Issue 69 (20 Feb 1990)
 - <u>A320 accident (Nancy Leveson, George Michaelson)</u>
 - Ferry line replaces "sail-by-wire" with pneumatic controls (Jon Jacky)
 - Now Prodigy Can Read You (Donald B Wechsler)
 - 3 KGB Wily Hackers convicted, mild sentences (Klaus Brunnstein)
 - Problems/risks due to programming language, stories requested. [Item Includes AT&T "do...while"..."switch"..."if"..."break" tale] (Gerald Baumgartner)
 - AT&T Says New Goof Wiped Out Many Toll-Free Calls (David B. Benson)
 - Re: Computerized Collect Calls (Adam Gaffin via Mark Brader)
 - RISKS of ANI blocking (James C Blasius)
 - <u>"Brilliant Pebbles" (Gary Chapman)</u>
- Volume 9 Issue 70 (23 Feb 1990)

Neutron reactor lands in hot water (Steve Strassmann)

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

Volume 9 Issue 71 (26 Feb 1990)

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

Volume 9 Issue 72 (28 Feb 1990)

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

Volume 9 Issue 73 (6 Mar 1990)

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

Volume 9 Issue 74 (12 Mar 1990)

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

Volume 9 Issue 75 (15 Mar 1990)

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

Volume 9 Issue 76 (19 Mar 1990)

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

Volume 9 Issue 77 (21 Mar 1990)

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

Volume 9 Issue 78 (5 Apr 1990)

- RAF Tornado collision (Dorothy R. Graham via PGN)
- New Georgia Automobile Tags (Warren Tucker)
- British tax tales (Bob Gray via Mark Brader)
- Oslo Day in Norway? No way! (Paul Dorey)
- Computer backorder on cover letters (Yuri Rubinsky)
- London Underground driver's action (Martyn Ould)
- Hi-Tech Loo (Wayne W. Lui via Brian Randell)
- Proposed UK Authority for Risk Management (Brian Randell) [See Box for cases]
- More on Prodigy's Updating of a User's Disks (Eric Roskos, Paul Eggert)
- April Fools Day on the net (D. Waitzman via Martin Minow)
- <u>Automated Fast Food (Dave Curry)</u>
- <u>UNIX Trix (Paul Eggert)</u>
- Re: PSU Hackers thwarted (Pete Mellor)
- Three Australians indicted for computer tampering (PGN)
- Volume 9 Issue 79 (9 Apr 1990)
 - Fixing Computer Error Cost \$1,300 in Overtime (Chris McDonald)
 - Computer problem delays Calif. Lotto payouts (Rodney Hoffman)
 - <u>Computer Glitch Cuts of Decco Sales (Mark Adams)</u>
 - Computer Animations in court testimony (Peter Scott)
 - Re: Proposed UK Authority for Risk Management (Dan Franklin)
 - Re: Intruders arrested (Mike McBain via Lee Naish)
 - Re: More on Prodigy's Updating of a User's Disks (Leonard Erickson)

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

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

Volume 9 Issue 86 (30 April 1990)

- Futures market shut down (Steve Bellovin)
- Habsheim A320 crash (Clive Feather)
- Throttle Hitch Hits 747-400 (Robert Dorsett)
- Re: Unattended Plane Take-off (Jan I Wolitzky)
- Re: Computers and names with special characters (Mike Van Pelt)
- Inadequate documentation truncated GPAs (Doug Sewell)
- "The return of the hacker" (David B. Benson)
- Indian Professors Teaching Virus Writing (Cliff Stoll)
- (Not necessarily) computer parks hundreds of cars illegally (Bill Gunshannon)
- Volume 9 Issue 87 (1 May 1990)
 - Phones & techologically illiterate operators (David A. Honig)
 - More telephone problems -- union pressures (Peter Jones)
 - Forwarding: Weird phone bills an unexplored possibility (Chaz Heritage via Richard Busch)
 - <u>Re: Call Forwarding (Peter Jones)</u>
 - Kissimmee Kate (Geoffrey H. Cooper)
 - <u>Re: You think YOU have problems with your telephone company? (Gary Cattarin, Jozsef A Toth, Warren Levy)</u>
 - Blaming it on the computer? (Brad Templeton)
 - Re: Risky McDonald's comrade... (Charles Youman)
- Volume 9 Issue 88 (2 May 1990)
 - Booby-trapped contracted software (Tom Kopp)
 - Death rate inflated in St. Bruno area, health report finds (David Sherman)
 - Software Bug Causes Shuttle Countdown Hold at T-31 Seconds (Karl Lehenbauer)
 - Criticism of "Glass Cockpits" (1) and (2) (Martyn Thomas)
 - A320 Bangalore crash (Martyn Thomas)
 - A320 criticisms reported (Martyn Thomas)
 - Re: computer parks hundreds of cars illegally (Andrew E. Birner)
 - (Apparently) widespread problem with census 800 number (Timothy M. Wright)
 - Re: You think YOU have problems with your telephone company? (Chris Lewis)
 - Telephone switch problems (Webber)
 - White paper available: "Improving the Security of Your UNIX System" (Davy Curry)
 - Virus found in a game software on the market (Yoshio Oyanagi)
 - Re: Computers and names with special characters (Bandy)
- Volume 9 Issue 89 (7 May 1990)
 - A funny thing happened at the lottery office (Alan Hargreaves)

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

Volume 9 Issue 90 (10 May 1990)

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

Volume 9 Issue 91 (13 May 1990)

- Hubble Telescope pointing in the wrong direction (Raymond Chen)
- "Feds Pull Plug On Hackers" (James K. Huggins)
- Airline booking cancellation (Pete Mellor)
- Simple tone dialler bypasses British Telecom charging (Nigel Roberts)
- Risks of caller identification (David A. Honig)
- Avoiding ANI by Dialing 1-900 (Gary McClelland)
- Duplicate Mailings of RISKS 9.89 -- BITNET (Emmett Hogan)
- Re: Hazards of laser printers (Paul DuBois, Peter Jones)
- IFIP Conference Call for Papers (Rick Schlichting)
- CALL FOR PAPERS: Computing and Ethics (Donald Gotterbarn)
- Volume 9 Issue 92 (17 May 1990)
 - <u>Army chafes under Congress' robot weapons ban (Jon Jacky)</u>
 - Re: [London] Tube train leaves ... without its driver (Gavin Oddy)
 - Re: First Hubble Images Delayed To Conduct Focusing Tests (Karl Lehenbauer)
 - ANI for the criminal as well as the private citizen (Brad Templeton)
 - Computer Virus Solicitation (Andy Warinner)
 - Feds Pull Plug On Hackers (Bob Sutterfield, Rick Clark)
 - <u>Re: Military Viruses (Jim Vavrina via David Brierley)</u>
 - Re: Magnetic ID cards for all Israeli citizens (Amos Shapir)
 - Risks of Laser Printouts (David Tarabar)
- Volume 9 Issue 93 (21 May 1990)
 - Stamford CT 18-hour telephone switch outage affects 27,000 lines (PGN)
 - Irrational and nonvaledictory reasoning (PGN)
 - Crackdown on 1-900-STOPPER? (John M. Sulak)
 - P.T.U.U.I. (Robert Hardy, PGN)
 - Military Computer Virus Contract (Rory J. O'Connor)

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

Volume 9 Issue 94 (25 May 1990)

- More on Stamford CT Telephone Switch Outage (PGN)
- Duplicate RISKS mailings...SOLVED! (Emmett Hogan)
- Cross about CRIS (Crime Report information System) (Pete Mellor)
- Disk failures after extended shutdown (David Keppel)
- The Internet is growing up! (Scott Deerwester)
- Are government secrets safer if not classified? (Mary Culnan)
- <u>Risks of slandering ... in public forums [re: P.T.U.U.I.] (Tom Blinn)</u>
- A320 again (Nancy Leveson)
- M1 Air Crash Inquest (Brian Randell)
- Tempus Fugit -- Claremont Clock Tower Tick Talk (Brian Randell)
- Telephone network synchronization and NavSat (John T. Mulqueen via James Price Salsman via JC%RMC)
- National Geographic also wants me to move (Tim Kay)
- <u>Re: Irrational and nonvaledictory reasoning (John Chew)</u>
- Volume 9 Issue 95 (26 May 1990)
 - Possible Anti-Virus Legislation (Robert Smithmidford via Thomas Zmudzinski via Linda K. Perez)
 - Secure UNIX Infected? (Craig Harmer via Russ Davis via Linda K. Perez)
 - Follow-up on Fed Raids on Hackers (David Ruderman)
 - Crypto '90 conference, 11-15 August 1990, UC Santa Barbara (John Gilmore)
- Volume 9 Issue 96 (29 May 1990)
 - Roller Coaster Accident Blamed on Computer (Gary Wright)
 - ATMs robbed with no signs of tampering (Stephen W Thompson)
 - Bank deposits huge amount in account and blames owner! (Richard Muirden)
 - Risks in secure documents (David Fuller)
 - You Think YOU Have Trouble with Your Telephone Company? (Donald B. Wechsler)
 - Steve Jackson Games & A.B. 3280 (Brian Sherwood)
 - Re: Secure UNIX Infected? (Steve Bellovin, Henry Spencer)
 - Dereferencing Tim Kay's address (David Kuder)

Volume 9 Issue 97 (30 May 1990)

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

4 🕤 🕨 🥖 📝

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

Feeds

RSS 1.0 (full text) RSS 2.0 (full text) ATOM (full text) RDF feed WAP (latest issue) Simplified (latest issue)

Smartphone (latest issue) Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



Jaime Villacorte <jaime@tcville.hac.com> Wed, 6 Jun 90 09:08:04 PDT

The following appeared in an article by Tim Considine in the June 4, 1990 issue of Autoweek. It concerned the use of a new computerized scoring system manufactured by Dorian Industries, an Autralian electronics firm for use in the recent Indianapolis 500 race. "Data-1, as the system is known is arguably the most advanced and foolproof scoring system in the world. Well almost foolproof." [...]

"...all monitors went blank on Lap 130 of the race.

The cause of such a catastrophe: A laser printer ran out of paper and the system froze. A simple problem, but one that hadn't been simulated during testing.

However, while the monitors were blank, Data-1's computer kept collecting scoring and timing information, even though those in the tower couldn't gain access to it for a while.

Thus the last third of the Indianapolis 500 ended up being scored by 33 people with clipboards - the system used for the last nine years anyway and which USAC director of scoring and timing Art Graham had the foresight to retain as backup."

[All was not lost though...the computer eventually saved the day :-) ...]

"Ironically, a mistake was made. In provisional results released immediately after the race, Eddie Cheever was seventh and Scott Brayton eight. But a half-hour later, the positions were reversed when Data-1's complete scoring data was fed back into the computer and the error was found and corrected - Brayton hadn't been credited with a lap he'd completed.

And not only had the new technology proven itself, but for the first time in memory, Graham and his crew finished in time for dinner."

- jaime villacorte jaime@tcville.hac.com

Hughes Aircraft Co, EDSG, POB 902, EO/E52/D203, El Segundo, CA. 90245 (213) 616-8954

Muclear hair-trigger still set (Johnson v. Chain)

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Tue, 5 Jun 90 14:34:52 PDT

On June 4, 1990, Soviet premier Gorbachev told a Stanford audience that the cold war was behind us. On the same day, Stanford computer manager Clifford Johnson filed his appeal brief in the Ninth Circuit Court of Appeals in San Francisco, case 90-15276, arguing that he had "standing" to sue General Chain, the Commander-In-Chief of the Strategic Air Command, to reduce the risk of accidental launch of Minuteman and MX missiles.

The appeal is from a District Court dismissal of the lawsuit Johnson v. Chain, et al., case C-89-20265-SW, filed May 1, 1989. The suit challenges "standing orders" that assure the immediate launch of Minuteman and MX missiles, at all times. Missile launch crews and their commanders are on perpetual alert, at DEFCON (DEFense CONdition code) 4, instead of the peacetime level of DEFCON 5. Johnson contends that this nuclear alert gives rise an ongoing risk of accidental nuclear launch due to computer-related error, a charge endorsed by Computer Professionals for Social Responsibility. Ultimately, Johnson seeks a declaration that the standing orders are illegal under constitutional, statutory, and international law, as follows:

- (a) in peacetime, based on Congress' required power to declare war, and on prohibitions against jeopardizing the peace;
- (b) prior to an actual first nuclear use and without express congressional authorization, based on the required power of Congress to qualitatively expand war, and on prohibitions against disproportionate response;
- (c) at any time, on grounds that they surrender to computers all-important war powers, and so constitute an unrepublican form of government; and
- (d) at any time, as they require subdelegation to military commanders of the decision to launch a nuclear strike, which is barred by the Atomic Energy Act and by the republican principle of the civilian supremacy.

Taking as true all the factual allegations of risk, the trial court dismissed the action on the ground that Johnson lacked "standing" to sue the government. The issues raised in the brief are as follows:

THE ISSUES ON APPEAL

GIVEN present and continuing computer-related risks of sudden accidental death to millions, and to the Plaintiff in particular, due to the Defendants' standing orders re the launch of nuclear missiles;

WHERE said standing orders are challenged as inherently reckless and in excess of authority under constitutional, statutory, treaty, and international law;

WHETHER, under Article III of the Constitution, the Plaintiff has standing to sue Defendants, either in their official capacities or as individuals, on the grounds that Defendants' conduct:

1. immediately endangers Plaintiff's life, and diminishes its daily quality, without due process, in violation of Fifth Amendment to the Constitution; and/or

2. is heedless of the dictate of the public conscience and/or constitutes a crime against the peace, which Plaintiff is specially qualified to complain of, so that his standing is assured, respectively, by the Martens clause of the Hague Convention Respecting the Laws and Customs of War on Land (1907) 36 Stat. 2277 and/or by Article 6(a) of the Treaty of London (1945) 59 Stat 1544; and/or

3. delegates to error-prone, computer-governed military drills ultimate political judgments, imposing upon the Plaintiff a here-and-now subservience to unrepublican government, in violation of Article IV z 4 of the Constitution.

The brief is 50-pages long, and dense with footnotes. It claims that the immediate threat of harm, imposed without due process, is an injury sufficient for standing, even though it is "pervasively shared." It also argues that Johnson's injury is particular, in that he works close to a top-priority target, namely, Sunnyvale's Satellite Control Facility, and in that, as a British citizen, he has no remedy through the ballot box. Besides, as an expert on the relevant technology, he has standing to complain of crimes against the peace under international law, even if he himself were not injured. Finally, the case is novel in asserting that the de facto delegation of political decisions to computers amounts to unrepublican government, and is actionable.

The government has thirty days in which to respond.

Metwork follies

Tim Shimeall <shimeall@cs.nps.navy.mil> Wed, 6 Jun 90 09:12:44 PDT

For reasons known only to them, the folks who run the MILNET/Arpanet gateways decided to sever the connections at about 9:00am Monday, and reconnect them at about 4:00pm Tuesday (both times PDT). Naturally, they gave no advance (or following) notice of these actions. (At least, neither our users nor our system administrators received such notice...)

It is unfortunate that the gateway administrators act with such apparent disregard for the users and such apparent capriciousness. Tim Shimeall

Ke: The A320's attacks of nerves (<u>RISKS-10.02</u>)

Danny Cohen <OHEN@ISI.EDU> Wed 6 Jun 90 14:43:21-PDT

About the A320'S ATTACKS OF NERVES

Mr. Bertrand Bonneau (the translator to English) did a terrific job of translation, given his knowledge of the subject area. Too bad that the original writer is not more knowledgeable of aviation.

For example, I was very surprised by the total absence of any reference to the B767/B767 with their glass cockpits and computers.

The main point of this article is that the procedures were bad, and that the French FAA was conducting the investigation rather than the French Department of Justice. Even if the French judges are only ten times technically-smarter than ours and if the French-FAA is only ten times more corrupted than ours, I'd still rather see their FAA, not their DoJ conduct the investigation. The article asks (in the sub-headline): "How could the willingness to declare the pilots responsible for major accidents, EVEN BEFORE THE JUDGES HAVE RETURNED THEIR VERDICT, appear other than suspect?" Sure sounds like a good question. Well, in the US the NTSB (and the FAA) typically have "probable cause" within a day, even though investigations take many months or even years. Is it suspect, too?

For example, the Aloha B737 experienced an explosive decompression on 28-Apr-88, and the NTSB report about it was submitted only on Jun-14-89, nearly 14 months later. However, within a day or two after accident everyone was told what happened. Was this suspect, too? Neither Boeing nor RISKS complained about it. I couldn't find the contribution in RISKS saying that:

How could the willingness to declare the aircraft responsible for this accidents, even before the judges have returned their verdict, appear other than suspect?

Another example, closer to our hearts: the article says "For example, the software in the flight warning computer [FWC] included a fault which a good computer scientist could have repaired without a doubt".

I take it to imply that this shows that because of "*Industrial Secrets*" (which cover the software) the operating airlines could not use any "good computer scientist" to simply go ahead and fix that fault. If this is the case -- how about all the regression testing that ANY change in operational flight software must go through? who would be responsible for the modified code? etc., etc.

To sum it up: opinionated reporting may leave something to be desired.

Danny

Ke: Article on A320 in Aeronautique, April 1990

Pete Mellor <pm@cs.city.ac.uk> Tue, 5 Jun 90 21:03:03 PDT

In <u>RISKS-10.04</u>, livesey@Eng.Sun.COM criticises my recommendation of the Aeronautique article, as follows:

> Writing of a translated article, he recommends it to us on several ground,> one of which is

>

<> b) the fact that it presents a French (and therefore not negatively biased?) <> view,

>

> The two problems with this are, first, Airbus is not exclusively a French> aeroplane. It is a joint venture between several European countries.

>

> Secondly, there has been quite a lot of negative comment about Airbus from > French sources, mainly from pilots' unions. Quite correct on both counts! The umbrella company, Airbus Industrie, is, however, based in France, and the company responsible for the EFCS, at which much of the criticism has been levelled, is Aerospatiale, also French. The representatives of these companies have made extravagant claims for the safety and reliability of the A320 EFCS in TV interviews (see quotes from the Equinox programme on fly-by-wire in <u>RISKS-9.42</u>). I am very well aware of some of the criticisms from French sources, but when I wrote the above, I was thinking of this fairly vociferous defence of the FBW concept in general, and A320 in particular.

(On the other hand, criticism emanating from the vicinity of Boeing, for example, *might* be expected to be a little bit biased. :-)

> The risk here is that of giving one source extra credence on specious grounds.

Yes, it is only one source, but *did* seem to be fairly well informed. If any RISKS or Aeronatics digest readers can fault the article technically, I would be very glad to hear from them.

One thing in my recommendation which *was* misleading was my carelessly worded statement that the author had drawn some fascinating conclusions about the cause of the Mulhouse-Habsheim accident. He had not, of course. He merely raised a few fascinating questions.

Other than that, please judge for yourselves, and read again my disclaimer :-).

Pete Mellor

A 320 article in Aeronautique

&tkielski.TDS-ASF@SYSTEM-M.PHX.BULL.COM> Wed, 6 Jun 90 01:01 MST

Minor erratum: This article actually appears in the "Aeronautique" section of the French science magazine "Science & Vie," in the April, 1990 issue. A rebuttal from Bernard Ziegler, technical director of Airbus Industrie, may be found in the following May issue.

"Computer to track down drivers without insurance"

<seanf@sco.UUCP> Sun Jun 3 13:27:33 1990

[This is from clari.tw.computers.]

BOSTON (UPI) -- Tens of thousands of illegally uninsured drivers in Massachusetts will be tracked down and hunted when the Registry of Motor Vehicles implements a new computer-based system beginning Friday.

The new system, which allows insurance companies to electronically send the Registry's computer a list of uninsured motorists whose policies have been revoked for nonpayment, aims at cracking down on the estimated 300,000 Massachusetts drivers who take to the roads without insurance. [...] Police will pursue those individuals who fail to obtain o insurance after being discovered.

[end excerpt]

I think the risks are obvious.

Another egregious database

elroy <marka@dsinet.UUCP> 4 Jun 90 21:11:15 GMT

Reprinted from the June 3rd 1990 Seattle Times:

"Computer-data program to link student with prospective boss" Newhouse News Service Lawrence Township, N.J.

Imagine if an employer could find out how many times a prospective employee had been late for school, or if a business could tap into a pool of high school graduates and find the model employee.

Those are among the possible uses of an information system being developed by the Educational Testing Services, the nonprofit institution that administers the college entrance exams.

Called Worklink, the program is designed to connect education and business by gathering information from student records and providing it to employers through a computer data bank.

The idea, according to George Elford of ETS, is to improve the work force by motivating students, particularly those who might lack the contacts to land a good job.

Ideally, cost for the program would be shared by schools and businesses - not the students. Elford says, since it aims to help students who lack traditional means of "getting a foot in the door".

"Because the advantages of social networks and family influences are reduced with Worklink, the socially disadvantaged will gain real benefits," Elford says.

"Students will be competing on their record, not on their ability to create an impressive resume. And because the data bank will include teacher ratings, letters of recommendation and previous work experience, Wordlink will avoid the problems of standardized tests that often compare the disadvantaged with the advantaged."

Under the voluntary program, everything from prose reading and document reading to punctuality would be assessed and, subject to student approval, entered into

the student's record. Such control would be exercised in order to build on an individual's strengths, says Elford.

The absence of criteria like punctuality might be noticed, however, just as vital information omitted from a resume would be, he adds.

If the system is successful, says Elford, it would provide an incentive for apathetic students to do well.

"Worklink, when widely used by employers, is likely to motivate students to develop and demonstrate their proficiency in a number of areas," he says. "This increased motivation is likely to lead students to view teachers and class work as a means to help them build a strong record. Now, kids (who are not applying to colleges) know nobody cares what they're doing in high school, so why work hard? ... Hopefully this would serve as an incentive."

While the reward for the student would be a good job, employers would benefit by having a competent work force at their fingertips.

Pilot projects for Worklink will be launched in Tampa, Fla., and Spokane, Wa. this fall if business leaders in those communities agree to cooperate, says Elford.

It will be at least a couple of years before the results of the pilot are known, but Elford hopes Worklink will eventually catch on throughout the country.

"I'd like to see this kind of record system used in most localities in 10 years," he says. "Our hope is this will raise the whole level of attainment in schools and in the workplace."

[Now let's see... ETS's standardized tests are no good, so they want to add an even MORE intrusive system. Is it just me, or does anyone else have a problem with this?]

Mark Anacker, Digital Systems International, Inc., Redmond WA USA (206)881-7544

Kisks of Caller Identification (Re: Lesher, <u>RISKS-10.04</u>)

David desJardins <desj%idacrd@Princeton.EDU> Tue, 5 Jun 90 23:26:25 EDT

From: David Lesher <wb8foz@mthvax.cs.miami.edu> > Given the level of violence within the general population around > here, the CID block seems to made a classic RISKS mistake. A system > designed for less critical use has been thrust beyond its design > parameters into a life-dependent role.

I think you are misplacing the blame. Anyone who chooses to have their life depend on call blocking deserves what they get. (As you point out, the call blocking isn't useful for those trying to conceal their law-enforcement relationship in any case.) If you walk up to my door and knock, I can find out who you are (by taking a photograph through my peephole). So logically police informants don't expect to be able to walk up to doors anonymously. Neither should they expect to be able to enter homes via telephone anonymously.

-- David desJardins

KE: Denial of service due to switch misconfiguration

&ilgallen.Catwalk@DOCKMASTER.NCSC.MIL> Wed, 6 Jun 90 18:49 EDT

In <u>RISKS DIGEST 10.01</u>, Marc Horowitz writes:

> It turns out, that as a "client," MIT doesn't get automatic updates
 >when new exchanges are created. Without this information, the switch has no
 >clue how to bill the caller, or even if it should let the caller make the call.
 >So it assumes the worst case, and disallows anyone from making the call. The
 >switch had to be manually programmed with the necessary information about the
 >new exchange.

This problem is not restricted to organizations which run their own switch, or those with an ESS. There are *lots* of plain ordinary PBX's in this divested world which have automatic "route selection" to decide whether to send that outbound call over normal or WATS circuits, and in my experience these often don't get updated with new exchange codes, so calls simply cannot be made in the absence of routing information. In at least one of these cases the PBX was one maintained by AT&T, which apparently did not have good communications with its former child, New England Telephone.

But wait, there's more ...

I had a problem when I first got a cellular phone (as soon as they were offered in Boston). Well, there was the aforementioned problem that PBX's had not been loaded with information about the new cellular exchange codes. But also, I found that I could not forward calls from a residential phone to the new exchange. Sure enough, the ESS run by New England Telephone had not been updated with information on how to forward to exchanges run by a "different" company, NYNEX Mobile Communications (both companies are owned by NYNEX).

Larry Kilgallen

Private mail on BBSes...

David Gursky <dmg@lid.mitre.org> Mon, 4 Jun 90 14:50:06 EDT

In <u>Risks 10.03</u>, nazgul@alphalpha.com (Kee Hinckley) poses some questions on handling private mail on BBSes that deal with illegal activities (the messages that is, not the BBSes in general).

It is true that as a Sysop, you can't legally read private mail to others. The loophole is you can read public mail. What many BBSes here in the Washington area do is (1) prohibit private mail, except to and from the Sysop or (2) put up up a public notice announcing there is no private mail on the BBS, only public and semi-private, and the Sysop reserves the right to inspect (read) all messages. Should a prospective used not be willing to abide by either (1) or (2), they need not use the BBS.

🗡 Re: 2600 article

<henry@zoo.toronto.edu> Mon, 4 Jun 90 12:43:53 EDT

>...suggests that I can be arrested based on the contents/usage of my
>BBS, even when I'm unaware of that usage...
>...it seems to me that the Electronic Privacy Act prevents me from taking
>any actions which would let me prevent the misuse of my board...

The real problem here is that the courts are still fumbling with the question of whether electronic media are publishers or common carriers.

A publisher, e.g. of a newspaper, is very definitely responsible for what he prints, and cannot claim innocence just because he wasn't paying attention to what the reporters were writing that day. A common carrier, e.g. the phone company, merely provides communication services and bears no responsibility for the content of messages. Most electronic media fall in a vast gray area in between, and nobody can really predict how a major court case would go.

Eventually, precedents and legislation will settle things. Meanwhile, one should not be surprised if law-enforcement people assume the worst. Deciding who is guilty and who is innocent is the courts' job, not theirs. In the absence of solid rules (nonexistent as yet) and informed judgement (unlikely, given that most of them are computer-illiterate), they have few options. When they don't understand what's going on and the rulebook doesn't help, but there are definitely people being victimized, all they can do is arrest those who appear to be involved and hope they aren't too far wrong.

Henry Spencer at U of Toronto Zoology

uunet!attcan!utzoo!henry



Search RISKS using swish-e

Report problems with the web pages to the maintainer



🗡 Bei Mir ist es nicht schoen

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 7 Jun 1990 16:13:40 PDT

Sorry for the GermanoRussian pun, but the two Soviet cosmonauts aboard the space station Mir (= peace) for the past three months have been waiting for supplies to be brought up by the module Kristall, launched on 31 May, so that they may attempt to stay in space to attempt repairs of their Soyuz spacecraft (whose insulation was damaged on launch on 11 February). The conputer controlling the docking of Kristall with Mir shut down the docking operation two hours ahead of schedule yesterday. A Tass report speculates that the computer system might have detected a malfunction in one of the Kristall's orientation system engines. Keep an eye out for further details. [Source: San Francisco Chronicle, 7 June 1990, p. A20]

Ke: Network follies (Shimeall, <u>RISKS-10.05</u>)

<chowe@BBN.COM> Thu, 7 Jun 90 16:08:45 EDT

I'm sure someone must have already replied to you about this, but what they probably were doing were reconfiguring to deal with the fact that the Arpanet was decommissioned on June 1. There is no more Arpanet. You were probably rerouted to your local regional net, which in turn is gatewayed to other networks, thereby making it apparent that the Arpanet is "back". But rest assured, the Arpanet is dead.

Carl

[THE ARPANET IS DEAD. LONG LIVE THE ARPANET. PGN]

Mitnet FTP-ing of back issues

<ERCEDES@IRMUNISA.BITNET> Thu, 7 Jun 90 06:04:01 -0700

At last I have discovered a way to get back issues of RISKS-Forum via BITNET. I think it could be interesting for you: BITFTP at PUCC is the e-mail address to get FTP-BITNET redirection. You shuld send a message like this to BITFTP:

ftp CRVAX.sri.com login anonymous cd sys\$user2:[risks] get risks-i.j [for some legitimate values of i and j, obviously] quit

Please note that connection to CRVAX.sri.com is allowed only after 7 PM. After a while, BITFTP replies with a session log and, if the file has been succesfully retrieved, will send the file itself.

Ρ.

Paolo Mattiangeli, Universit{ di Roma "La Sapienza", Dipartimento di Fisica N.E., P.le Aldo Moro, 4 - 00185 Roma Italy

Kisk is in the eye of the beholder?

<rwex@ida.org> Thu, 07 Jun 90 14:44:08 E+1

At a briefing today, we were given information about the ATF (advanced tactical fighter) reported to be "tip-top secret."

(ATF is a highly automated plane that will eventually -- one is told --

house the Pilot's Assistant, an AI package that can fly, land, and fight the plane under every circumstance. Right. Anyway...)

The ATF has two cockpits. In the front one is a man. In the back one is a dog. The responsibility of the man is to turn around periodically and feed the dog. The responsibility of the dog is to bite the man if he ever tries to touch any of the controls.

Well, it seemed funny at the time.

--Dick Wexelblat
[We seem to be specializing in old shaggy dog stories. PGN]

Re: The A320's attacks of nerves (<u>RISKS-10.02</u>)

Robert Dorsett <rdd@rascal.ics.utexas.edu> Wed, 6 Jun 90 22:52:05 CDT

> Mr. Bertrand Bonneau (the translator to English)

Actually, Mr. Mellor did the translation. [Yes, that's what he said in <u>RISKS-10.02</u>. PGN]

>For example, I was very surprised by the total absence of any reference >to the B7[5]7/B767 with their glass cockpits and computers.

The B757/767 and A320 are two different generations of aircraft. And nobody's crashed a 757/767 yet. The airplanes could certainly come in for criticism (for the way Boeing's addressed the general man-machine problems of glass cockpits), but the *critical* issue of the day is the A320.

Looks like it's time for some refresher background:

757, 767, and A310: introduced in '82 and '83: characterized by *conventional* flight controls, glass artificial horizons and nav displays (EFIS), and performance management systems (PMS). These airplanes are referred to as "classical glass" by at least one magazine (Flight International).

The 757 and 767 have identical cockpits. They have conventional (analog dial) airspeed, altitude, vertical speed, and VOR/ADF indicators. These surround the two glass EFIS CRT's to form the "classic T." Engine monitoring is accomplished through an Engine Indication Control Advisory (EICAS) system, which is comprised of a primary flight instrumentation display (engine power, temperature, etc) and a secondary advisory display (checklists, hints, systems info, etc. pop up). These are stacked on top of each other on the center console. Boeing's operational cockpit philosophy, since the early 1970's, has been "need to know." The 757/767 represent the most extreme manifestation of this philosophy, by any manufacturer, to date. The implementation has resulted in the *necessity* of pilots having to work around system obstacles, by pulling circuit breakers (one source claims that on a

typical 767 flight, sixty CB's are set and reset). Data from an (unpublished?) survey by Earl Wiener indicates that pilots are neatly divided in their opinions of the 757/767 cockpit.

The A310 is similar, except it packs more info into the EFIS displays, and it has conventional dial engine instruments. However, it also has two EICAS displays, to handle a multitude of system and advisory information. Airbus's philosophy (on the A310) was "nice to know." The cockpit is not, however, popular with pilots, because of a variety of environmental factors (too cold, for one). There is a retrofit which gives the A300-600 more or less the A310's cockpit. The A320 design leans more in the 757/767 direction.

Next generation: the A320 (introduced in 1988).

The A320 did away with most dials (except for backup instrumentation) and combined airspeed and altitude information into the primary flight display. These bracket (left and right, respectively) the artificial horizon display. The display is quite small (7.25"), and, in my opinion, poorly designed (this was recently discussed ad nauseum on RISKS and sci.aeronautics). The nav display (beneath it) is more or less a typical nav display. Nothing revolutionary there.

The flight controls on the A320 are non-standard. The aircraft is controlled through sidesticks, which map pilot commands into aircraft action. There are a multitude of control modes available (for instance, "direct" mode, in which the sidestick deflections map to surface deflections), "autopilot" (in which the sidestick controls the autopilot), "C*" (which provides an unconventional method of flight guidance), etc. There are also many "protections" built into the various modes, such as automatic engine spool-up if the angle of attack gets too high (alpha floor--but it doesn't work under 100' radio altitude, hence the Habsheim crash), preventing excessive bank or pitch, etc. The two sidesticks do not provide "active" artificial feel (although they do have a spring to prevent excessive deflection), and are not interconnected.

There are manual backups to the flight control system, but they're not intended for normal use. The "manual" backups amount to electric trim, a manual rudder, and, according to at least one source, a manually settable horizontal stabilizer. At least one source has claimed that Airbus isn't advocating training for the "manual" flight mode, despite it being the only way that a test flight (which Bev Littlewood recently mentioned) could have been landed.

Latest generation: MD-11/747-400.

The MD-11 (1990) and 747-400 (1989) feature six large color CRT displays, and provide data in a manner similar to that of the A320 and 757/767. The MD-11 features a "fly-by-wire" system (without any changes in control laws and no protections), with a fully "manual" hydraulic backup. The 747-400 features a standard hydraulic-based control system. Both airplanes are two-man ships, though, and include significantly reworked electrical and systems design.

Note, though, that both Boeing and McDonnell-Douglas have opted for *conventional* flight laws. Boeing is reportedly continuing the trend

with the 767-X (777), which, if launched, will have fiber-optic "fly-by-light" systems.

In essence, these airplanes share (a) similar nav displays, (b) similar PMS/FMCS systems, (c) similar (unknown) problems relating to the consequences of using digital electronics for flight-critical systems (these range from static problems to temperature to solar radiation), (d) the unknown effects of "hiding" a lot of information in two little CRT's, and (e) a propensity to encourage "heads-down" behavior. Only the A320, however, has a fly-by-wire system with "unconventional" control laws, and only the A320 has been sold on the basis of preventing the pilot from making fatal errors.

As you note, though,

>The main point of this article is that the procedures were bad,

which brings us back to ERGONOMICS. The point of the article was to draw attention to the questionable workmanship of the aircraft, and the poor man-machine interface. In my opinion, the A320 is the real loser in the crop of digital airplanes, with the 747-400/MD-11 coming a distant second (for the idiotic decision to introduce long-range aircraft with only two pilots).

>the French FAA was conducting the investigation rather than the French >Department of Justice.

Actually, both the DGCA and a local magistrate were conducting an investigation. The DGCA has released its report, which white-washed the aircraft and systems. The magistrate's report is still to be released (?).

>Even if the French judges are only ten times
>technically-smarter than ours and if the French-FAA is only ten times
>more corrupted than ours, I'd still rather see their FAA, not their DoJ
>conduct the investigation.

But there's an explicit conflict of interest there: Airbus Industrie is essentially a public-works project for the aerospace sector in Europe. It is HEAVILY financed by the French government, and is a major employer in France. French prestige is on the line, and we all know how "weird" the French government can get, when protecting its interests (remember the Rainbow Warrior? :-)). The behavior of both the French government after Habsheim, and Airbus Industrie after Bangalore, are certainly bases for skepticism.

>Well, in the US the NTSB (and the FAA) >typically have "probable cause" within a day, even though investigations >take many months or even years. Is it suspect, too?

There are numerous cases when the NTSB has not been able to issue a probable cause, and numerous more where the probable cause has turned out to be incorrect. What the French government did, however, was state--in a definitive manner--that the Habsheim crash was a result of pilot error. The FORM their statement took would certainly not be acceptable coming from the NTSB. It must be very awkward to have a supposedly objective government agency immediately *defending* an airplane of which many hard questions can be asked. It's my impression that what irked many people was this very sight of their government playing the role of apologist.

To the best of my knowledge, the FAA does not issue probable-cause statements. Its options are limited to emergency regulatory action, based upon preliminary crash assessments from the NTSB (cf. the AAL DC-10 at O'Hare). It, too, has been known to reverse its decisions.

>To sum it up: opinionated reporting may leave something to be desired.

The style of the article was somewhat clumsy, but it has a number of good points. It is not appropriate to discount it sorely because of its feeble attempts at rhetoric. A number of people seem to have been thrown off by the assumption that it represents the epitome of the debate in France. It doesn't, as Pete Mellor has noted. But it certainly contains enough (apocryphal) anecdotes to stimulate serious discussion.

Robert DorsettModerator,Internet: rdd@rascal.ics.utexas.eduAeronautics DigestUUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

Ke: The A320's attacks of nerves (Cohen, <u>RISKS-10.05</u>)

Steven Philipson <stevenp@decpa.pa.dec.com> Thu, 7 Jun 90 15:26:06 PDT

In <u>RISKS 10.05</u>, Danny Cohen <OHEN@ISI.EDU> made some statements regarding accident investigation in the US that are not correct.

> [...] Well, in the US the NTSB (and the FAA)
 > typically have "probable cause" within a day, even though investigations
 > take many months or even years. Is it suspect, too?

The FAA *never* issues statements of probable cause -- it is outside its jurisdiction. The NTSB has primary jurisdiction. The role of the FAA in accident investigation is to collect facts and assist the NTSB in their investigation of accidents. Probable cause statements are issued by the NTSB in accident reports that typically are released about six months after the accident. NTSB board members will on occasion issue statements about the focus of investigation, and about preliminary findings, but official statements are not made until exhaustive study is complete and the accident report is completed. Safety recommendations can be made more expeditiously when an urgent need is perceived, but this is not equivalent to a statement of probable cause. There would be a tremendous negative response to a Board member if he/she made such a statement within a day, and indeed, such a statement would be suspect. Just for fun, I challenge all RISKS readers to find a single case wherein such a statement was made "within a day". In the case of the Aloha accident certain facts were known fairly quickly. Recommendations were made to the FAA to address perceived safety problems, but no statement of probable cause was issued until the official report was released.

>To sum it up: opinionated reporting may leave something to be desired.

Granted. The same can be said of misinformed reporting.

Steve Philipson

Ke: Article on A320 (Mellor, <u>RISKS-10.02</u>)

Karl Swartz <kls@ditka.UUCP> 4 Jun 90 02:21:46 PDT (Mon)

I don't have definitive answers, but I think I can clarify the terms a bit. "About-turn on the ground" is an abort before the beginning of the takeoff roll, that is, a decision to return during the pre-takeoff taxiing, whereas an "acceleration-stop" is an abort after the beginning of the takeoff roll but before V1 (the velocity at which the plane is committed to a takeoff) is attained. The latter is an aborted takeoff; beyond V1 the plane is committed to a takeoff though once airborne the crew could immediately turn back and land.

As for the matter of "cabin altitude being on the increase", pressure in the cabin is measured in terms of altitude rather than PSI or bars or some other unit. Typically, the cabin of a commercial aircraft is pressurized to a pressure equal to that at an altitude of 8,000 feet above mean sea level. A failure of the pressurization system would cause the pressure to decrease such that the effective cabin altitude would increase from nominal, approaching the actual altitude of the aircraft. Often this occurs due to a rupture of the pressure cabin and a consequent violent decompression, but in this case it appears the decompression was gradual, presumably due to a failure of the regulation systems. No matter, the pilots still must descend to an altitude at which the cabin altitude is within acceptable limits.

Karl Swartz, 1738 Deer Creek Ct., San Jose CA 95148 1-408/223-1308

A320 - The Attacks Continue

Pete Mellor <pm@cs.city.ac.uk> Thu, 7 Jun 90 20:33:41 PDT

In <u>RISKS-10.05</u>, Danny Cohen <OHEN@ISI.EDU> writes:

> About the A320'S ATTACKS OF NERVES

> Mr. Bertrand Bonneau (the translator to English) did a terrific job of
 > translation, given his knowledge of the subject area. Too bad that the
 > original writer is not more knowledgeable of aviation.

If this is a joke about the translation, it's a bit too subtle for me! My Collins-Robert French Dictionary gives:

"crise de nerfs - attack of nerves, fit of hysterics;"

Mmm...perhaps the second alternative might be better :-) Assuming from the lack of smiley that Danny Cohen is serious, then he can't have read my disclaimer.

He goes on:

> For example, I was very surprised by the total absence of any reference> to the B767/B767 with their glass cockpits and computers.

Maybe, but M. Bonneau *does* say "...the embedding of numerous pieces of software on board aircraft of the new generation (A320, but also McDonnell-Douglas MD 11, Boeing 747-400, among others) can pose problems for the official agencies.", so he is obviously aware that the A320 is not the only computerised civil aircraft.

> The main point of this article...

[Actually the main point of the subsection on the enquiry into the Mulhouse-Habsheim crash: the main article is far more concerned with technical problems of FBW and glass cockpits.]

...is that the procedures were bad, and that
 the French FAA was conducting the investigation rather than the French
 Department of Justice.

Err..not *quite*. Bonneau's point is that French government regulations (to which he gives precise references) place the responsibility for conducting such investigations on the Inspection Generale de l'Aviation Civile (IGAC), under the direct authority of the Minister of Transport [note: *not* the "French Department of Justice"], and not on the Direction Generale de l'Aviation Civile (DGAC), which is the French equivalent of the FAA.

The only information I previously had on alleged procedural irregularities came from some slightly confused accounts in the UK and US press (Herald Tribune 11th July 1988, Financial Times 11th July 1988, Guardian 12th July 1988, New Scientist 21st July 1988). It was Germain Sengelin, senior examining magistrate at Mulhouse, who complained at the DFDR and CVR being handed over to the DGAC without being placed under judicial seal to "guarantee their authenticity and integrity" until the enquiry. He was taken off the case.

> Well, in the US the NTSB (and the FAA)

> typically have "probable cause" within a day, even though investigations> take many months or even years. Is it suspect, too?

Depends. The pilot and copilot survived the Mulhouse crash, and immediately

made statements implicating delays in engine acceleration (Times 27th June 1988). The engines are controlled by FADEC, and this in turn responds to the EFCS. The question about exactly *what* goes onto the DFDR, and from *where* it is captured in the processing chain, had previously occurred to several people (including myself) who take an interest in the A320. If Bonneau's claims about this are correct, it confirms our suspicions: even *with* the information from the DFDR, it would not be possible to identify "pilot error" as the sole cause without other evidence. Metal fatigue in antique airframes (Aloha B737 28-Apr-88) is well understood as a cause of accident. Systematic failure of a complex FBW system is not. That, together with the statement of an experienced pilot that the engines did not respond to commands, make the following timetable look a bit like a "rush to judgement":

26th June, 1245: Mulhouse crash. DGAC takes control of DFDR and CVR.

26th June, evening: Air France and BA A320's grounded.

- 27th June: Louis Mermaz, French Minister of Transport, announces that analysis had shown the plane suffered no technical problems. (Guardian, 28th June)
- Same day: Jean Volff, local public prosecutor at Mulhouse, announces that "The inquiry points towards pilot error." and that "he could not exclude prosecution of the pilots for manslaughter if error is proved". (Guardian, 28th June, same article)
- Same day: BA reverses grounding decision after "it had discussed the situation with both the Civil Aviation Authority and manufacturers Airbus Industrie". (Evening Standard, 27th June)

28th June: A320's back in service.

The last event is the one that matters, of course. Bonneau's speculation that "... the concern of the only technical enquiry had overridden that of the judicial enquiry." may be true. The concern that overrode everything was to get the A320 back in the air.

>From the New Scientist, 21st July 1988:

"...the day after the accident, the DGAC announced a preliminary conclusion that the pilots, and not the aircraft, were to blame for the disaster. According to the French press, details of the flight records were given to Aerospatiale, which announced that it had confirmation that the aircraft was not at fault in the crash. Several days later, the DGAC exonerated the mechanical performance of the Airbus. The head of the DGAC, Daniel Tenenbaum, said that if this had not been the case, it would have been necessary to ground the A320 for tests."

(And we couldn't have that, now, could we? :-)

[In fairness, I should add that I have spoken to a number of people in the CAA and elsewhere who know a lot about flight certification and about the Mulhouse accident in particular, who have assured me that it *was* pilot error, but, as always, confidentiality prevented them from saying *how* they

knew that.]

> I take it to imply that this shows that because of "*Industrial
> Secrets*" (which cover the software) the operating airlines could not
> use any "good computer scientist" to simply go ahead and fix that fault.
> If this is the case -- how about all the regression testing ...

I agree. If Bonneau thinks that each user could hack together his own patches, then he's WRONG. He is, however, quite right to point out elsewhere that it's not possible to certify a system containing embedded software to any high degree of reliability (and certainly not to 10^-9) by treating it as a black box, and the industrial secrecy protecting the A320 software means that it is possible to do little else.

In fact the regulations (FAR 25.1309 plus AC 25.1309-1) require a "critical" *system* to be demonstrated to have 10^-9 max. probability of failure, but specifically 'cop out' when it comes to the *software* in those systems, and refer to RTCA/DO-178A, "Software Considerations in Airborne Systems and Equipment Certification", which is essentially a set of guidelines for good development practice, and requires that certain documents (specifications, test plans and results, etc.) be made available to the certification authority. There are 3 levels of software, of which level 1 is for "critical" systems (those which can crash the aircraft if they fail). (However, note that by "using appropriate design and/or implementation techniques" it may be possible to put lower level software in a critical system.) Even at level 1, source code and object code are *not* required, and a source listing is only required for a re-certification following modification! Only the vendor of the software and the customer (i.e. the airframe manufacturer) are required to test the software.

A320 EFCS software was rated as level 1. Heaven knows what's in the FADEC! (The European regulations are almost identical to the US.)

As a modest proposal for improving our certification of flight-critical software, may I suggest:

- Access to source and object code by certification authority.

- Independent Verification and Validation (IV&V) by 3rd party.

Danny Cohen ends:

> To sum it up: opinionated reporting may leave something to be desired.

To which I say: so may our certification procedures for flight-critical software!

Also in <u>RISKS-10.05</u>, Atkielski.TDS-ASF@SYSTEM-M.PHX.BULL.COM points out that the actual magazine is "Science & Vie", and that the article was in the "Aeronautique" section. Sorry, my fault. Serves me right for working from a photocopy of only the relevant pages.

He also points out that:

> A rebuttal from Bernard Ziegler, technical director> of Airbus Industrie, may be found in the following May issue.

My thanks for this information. Perhaps in the interests of balance, RISKS should carry a translation of that, too. Are you offering, Bernard? Come on, it's someone else's turn! :-)

My thanks also to Steven Philipson, Karl Swartz and Jordan Brown for answers to my queries about the terms "acceleration-stop", etc. Since Karl copied his reply to RISKS, I assume it will be appearing shortly.

Pete Mellor (Author of the above, but mere translator of Bertrand Bonneau's article!)

Ke: Private mail on BBSes...(and the A320?)

Pete Mellor <pm@cs.city.ac.uk> Thu, 7 Jun 90 20:53:21 PDT

With regard to David Gursky's points about BBS mail that deals with "illegal" activities, what if Airbus Industrie decides the Bertrand Bonneau's article is libellous. Do they sue the publishers of "Science & Vie", M. Bonneau, me, Peter G. Neumann, or all of us?

OK, RISKS is a moderated forum, so I suppose the buck ought to stop with the moderator. :-)

This problem reminds me, however, of the case of Goldsmith v. Pressdram (publishers of the UK magazine "Private Eye") a few years ago. Sir James Goldsmith sued Private Eye for libel. As part of his action, he also tried to sue the distributors and retailers of the magazine. This was thrown out, since if the precedent had been established, it would have meant that every newsagent and magazine stall-holder in the land would be expected to read every publication he sold from cover to cover, and be liable if he failed to withhold any issue that was libellous.

Doesn't a similar common-sense principle apply to (non-moderated) BBS's?

Pete Mellor

4 🛖 🕨 🗊 🖉 🐨 🚀

Search RISKS using swish-e

Report problems with the web pages to the maintainer



<LERCAMA@HEITUE5.BITNET> Thu, 7 Jun 90 11:53 N

Software protection debate in European Parliament in deadlock?

"If builders built houses the way programmers write programs, the first woodpecker coming along would destroy civilization"

(Anonymous, attributed to Murphy)

Following the proposed Community Directive on Software Protection of 1988 to which legislation in all twelve member states of the European Community should

adhere, various committees in the European Parliament have occupied themselves with the proposed regulations. Today, June 7, 1990, is a renewed and delayed deadline for submission of amendments to the Committee on Legal Affairs and Citizen's Rights who hope to come to an agreement on 18 and 19 June 1990. If agreement is reached, the final proposal will be submitted to the plenary meeting of the European Parliament in Strasbourg, France, to be voted upon during July 1990. However, there appears to be considerable disagreement on the proposed copyright exemptions under Article 5.

In the final report by the parliamentory Committee on Financial and Monetary Affairs and Industrial Policy (Draftsman: Mr K. Pinxten M.E.P., 22 March 1990, PE 134.05/fin.) to the Committee on Legal Affairs, the following copyright exemptions were proposed:

Article 5(1). Where a computer program has been made available to the public IN A LEGAL MANNER, the acts enumerated in Article 4(a) and (b) shall not require the authorization of the rightholder, in so far as they are necessary for the use OR SCIENTIFIC ANALYSIS OR TESTING of the program.

Article 5(2). Where a computer program has been made available to the public IN A LEGAL MANNER, THE RIGHTHOLDER MAY NOT PREVENT THE NORMAL USE OF THE PROGRAM BY THE PUBLIC IN PUBLIC LIBRARIES.

Article 5(3). A LICENCE AGREEMENT OR OTHER WRITTEN AGREEMENT MUST NOT CONTAIN ANY CLAUSES WHICH CONFLICT WITH THE PROVISIONS LAID DOWN IN PARAGRAPHS 1 AND 2.

The acts in Article 4 refer to copying, translation (assembling/compiling), viewing and running for normal operation of a `program' in, presumably, source, object, or executable form. Interestingly, the explanatory notes to these amendments dwell extensively on normal use, library exemptions, and the mandatory nature of these conditions, but not at all on the `scientific analysis and testing' provision as proposed for Article 5(1).

Under the Berne Author's Rights ('Copyright') Convention upon which the European Community wishes to base its Directive, personal CREATIVITY rather than engineering / corporate EFFORT determines whether a work is protected. It is in this respect that software quality and safety are at stake. Any creative activity is bound to be error prone (and especially so under competition-based time constraints), and it has only been since recently that this is being recognized by legislative and regulating bodies. In a recent U.S. report BUGS IN THE PROGRAM (*), a serious lack of testing norms for safety-critical software is apparent (e.g., aircraft control, medical equip ment),

"At the present level of understanding in software engineering, Federal agencies cannot be assured the software they oversee and use is correct; they CAN determine whether the software developer understands good practices that are necessary to produce quality software. Further, review and analysis and test results are useful, though this offers no safety guarantee."

If legislative and regulating bodies in a major software producing country like the U.S.A. recognize their limitations to assert software quality, it would seem that new regulations should provide room for such validation and

testing by others. One such a regulation might be the proposed amendment on analysis and testing, insofar it cannot be excluded by contract, AND insofar it extends to third parties like consumer societies and other investigating entities, including the right to publish the findings from such (scientific) endeavor.

(*) Bugs in the program -- Problems in Federal Government Computer Software Development and Regulation. Subcommittee on Investigations and Oversight to the Committee on Science, Space and Technology, U.S. House of Representatives, August 3, 1989 (submitted by James H. Paul, Staff Member and Gregory C. Simon, Staff Director and Councel). See also Michael Rogers & David L. Gonzalez, Can We Trust Our Software? Newsweek, 29 January 1990, pp. 42-44.

[Note: the library exemption does not seem to encompass the custom in many university computer centers that software can be borrowed by staff and students for exclusive use on local PC's]

Herman J. Woltring, CAMARC partner (NL) Brussellaan 29, NL-5628 TB Eindhoven The Netherlands, tel & fax +31.40.413744

CAMARC ("Computer Aided Movement Analysis in a Rehabilitation Context") is a project under the Advanced Informatics in Medicine action of the Commission of the European Communities (AIM/DG XIII-F/CEC), with academic, public-health, industrial, and independent partners from Italy, France, U.K. and The Netherlands. Its scope is pre-competitive.

Computer Aids May Hurt in Decision Making

Brad Dolan <pine_ridge@oak.span> Mon, 4 Jun 90 12:37:26 GMT

[From the _Wall Street Journal_; June 1, 1990, p. B1.]

COMPUTER AIDS MAY HURT IN DECISION MAKING

Computer programs designed to assist managers in making decisions don't always help, and sometimes can hamper performance, a team of researchers finds.

Jeffrey E Kottemann, assistant professor of computer information systems at the University of Michigan, simulated a manufacturing-production process in a growth industry. He had M.B.A. students decide on output and staffing, given uncertain demand, over 24 mock quarters. One group used a spreadsheet-oriented computer aid that helped members evaluate alternatives. The other group was on its own, relying on intuition and experience.

Contrary to Mr. Kottemann's expectations, the computer-assisted people significantly underperformed unaided, in the initial experiment as well as two follow-ups. With the computer aids, he says, people appear to have sought short-term results by understaffing and underproducing. But those decisions, over time, meant lost sales and extra costs.

Oddly, the computer-aided group didn't recognize that using the programs led to poor decisions. "They were significantly more confident in their performance than the unaided group," Mr. Kottermann says. He and two colleagues, Fred D. Davis Jr. and William Remus, plan further work to help explain when and how computer aids affect actual and perceived performance.

Brad Dolan Science Applications International Corp.

Ke: Another egregious database (Anacker, <u>RISKS-10.05</u>)

Steven Philipson <stevenp@decpa.pa.dec.com> Thu, 7 Jun 90 15:26:06 PDT

Mark Anacker (marka@dsinet.UUCP) writes about "Another egregious database".

The database that Mark reported on is not merely "egregious", but is excessively intrusive and constitutes a massive invasion of privacy as well.

The inventors of this scheme posit that closely kept records would motivate disadvantaged students to attend classes more regularly and strive harder to perform. There seems to be no basis for these claims. A more effective argument could be made such that such record keeping would discourage students -- any minor slip would be recorded and permanently held against them. The system would appear to be designed to hold them back, thus further alienating them from the school and society as a whole.

The data collected in this system could be used as a basis to disqualify or downgrade students for jobs and college acceptance based on their well-documented poor attendance, lack of motivation, and poor performance. Standardized tests provide some objective measure of skills and capabilities of students. This new system seems to provide a mechanism for rejecting students on more subjective grounds.

>If the system is successful, says Elford, it would provide an incentive for >apathetic students to do well.

This logic is backwards. The success of a tracking/incentive system should be judged on how well it motivates students and effects their learning. A perfectly implemented system that negatively effects the students cannot be considered a success.

>Is it just me, or does anyone else have a problem with this?

It's not just you. This proposal is offensive, and the article is amazingly blind to its problems. Hopefully the communities involved will do better. If not, perhaps they'll give it an appropriate name and slogan: Long Live Big Brother!

Steve Philipson

Re: Another egregious database (+ egregious student assessments)

Pete Mellor <pm@cs.city.ac.uk> Thu, 7 Jun 90 21:20:17 PDT

In <u>RISKS-10.05</u>, from the June 3rd 1990 Seattle Times, courtesy of Mark Anacker:

> Imagine if an employer could find out how many times a prospective employee
 > had been late for school, or if a business could tap into a pool of high
 > school graduates and find the model employee.

(Article about "Worklink, the program designed to connect education and business")

Who *wants* to employ these paragons? An article in New Society many years ago carried an article about how research grants were awarded. The discussions of an imaginary committee were reported, considering the following two cases:

Student A had hypochondriac tendencies, and a noted aversion to serious work. A completely undistinguished undergraduate career at Cambridge had been spent mainly indulging in drink and sport, apart from his hobby of collecting insects. He now wanted to go on a round-the-world cruise on some research ship with no well-defined research objectives whatsoever in mind.

Student B was rather withdrawn and given to boughts of introspection on obscure and irrelevant topics understood only by himself. His medical records reveal that he did not speak until the age of four. His habits were eccentric: he sometimes wore no socks, and had been caught wearing his landlady's tablecloth as a scarf. This general neurotic impression was confirmed by the fact that examinations reduced him to a state of nervous collapse for several months before and after. Since graduation, he had been employed as a clerk in a patents office.

Needless to say, the committee did consider either student worthy of an grant. Unfortunately, the first was Charles Darwin, and the second was Albert Einstein.

Still, we can't all be eccentric geniuses. If you want a reliable guy to serve on a burger stand, try Worklink! :-)

Pete Mellor

K Re: Another egregious database (<u>RISKS 10.05</u>)

Edwin Wiles <ewiles@iad-nxe.global-mis.dhl.com> Thu, 7 Jun 90 19:36:44 EDT

Yes, I too had a problem with this, until I ran across the following paragraph...

>Under the voluntary program, everything from prose reading and document

>reading to punctuality would be assessed and, subject to student approval,

^^^^

>entered into the student's record.

Since the program is voluntary, and the information in it is "subject to student approval", I have fewer problems with the database itself. Yes, unscrupulous school administrations could indeed enter data that the student had not aproved, but discovering this should be as easy as getting a copy of your school transcript is now. (It's VERY easy for me.)

However, all it has done is moved the 'disadvantage' from the "post-school" period (i.e. writing impressive resumes), to the "in-school" period (i.e. getting sufficient counseling to have 'impressive' data in your records). At my high school, this would have been something of a lost cause. There were only two counselors for the entire school. Fortunately, I was well motivated and already knew what I wanted, so I didn't need much counseling.

Youth has such an ability to disregard unpleasant consequences....

Edwin Wiles, NetExpress, Inc., 1953 Gallows Rd. Suite 300, Vienna, VA 22182

Ke: Risks of Caller Identification (Re: desJardins, <u>RISKS 10.05</u>)

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Thu, 07 Jun 90 12:59:12 PDT

David desJardins writes:

> If you walk up to my door and knock, I can find out who you are (by taking a
> photograph through my peephole). So logically police informants don't expect
> to be able to walk up to doors anonymously. Neither should they expect to be
> able to enter homes via telephone anonymously.

Let us be clear about who Caller ID benefits and who it does not benefit.

As far as residential phone users are concerned, Caller ID is not much better than receiving anonymous calls. That is, having the number of the calling phone is *not* sufficient information to decide how to handle the call, since the vast majority of calls will be from unrecognized numbers, which could just as easily be from a spouse stranded with a broken-down car as from a stranger. A real name -- a simple ascii string -- typed by the caller at call time or sent from a card that the caller placed in the calling phone, would be be far more useful to the callee for call screening purposes.

For businesses on the other hand, Caller ID is *much* better than receiving anonymous calls. That is because businesses want the number for a *different* reason than residential customers do: they aren't trying to screen calls; they are trying to collect marketing information. Thus, they need an ID that can serve as a link back to the caller. Phone numbers -- via reverse directories that are readilly accessible -- serve this purpose. For businesses, a simple string like "John" or even "Mergatroyd D. Fitzsimmons" wouldn't be useful because
it can't serve as a unique link back to the caller.

My preference would be to hold out for a solution that provides real benefits for residential users, and that does *not* provide benefits for businesses.

IJ

Ke: Steven Jackson Games (<u>RISKS-10.04</u>)

Jerry Leichter <leichter@LRW.COM> Thu, 7 Jun 90 09:43:30 EDT

In a recent RISKS, Jim Harkins (correctly) writes that we consider books containing all sorts of details about how to commit crimes to be legal. He then says:

I [haven't] done anything wrong by offering a suggestion on improving your monthly income [by holding up gas stations] :-) Of course, if I suspect that you did use my suggestion then by not finking on you I am breaking the law.

This last sentence is FALSE. You have, in general, no positive duty to report your knowledge of a crime, much less your suspicions. There are some special cases, mainly having to do with "officers of the court" or police; if you fall into one of these special categories, you should know. In fact, under some conditions your reports, if false, MIGHT be actionable as libel or slander. (There's a fine balance of interests here - society's interest in seeing crimes punished and, if possible prevented; and individuals' interest in seeing their privacy and "good name" protected. As an analogy - one where the "damage" is considered more severe - anyone has the right to make a "citizen's arrest" of the committer of a felony. But beware: If you exercise this right, you MUST be right in your claims! If the person you "arrest" did not in fact commit the felony you "arrested" him for, he can successfully sue you (probably for battery). That you BELIEVED he had committed a felony, even had very good reason for such a belief, is insufficient. This is one place where police officers have much, much broader lattitude than the average person.)

On the other side, one thing you have to watch out for in this context is conspiracy laws. These were great favorites for going after people unpopular with the authorities back during the anti-Vietnam-war protests of the '60's, since they are so broadly drafted. As I recall, if 2 (3?) or more people discuss an illegal act, and at least one of them then goes out and performs any concrete action in furtherance of that act, all can be found guilty of conspiracy, a crime for which the penalty can be more severe than that for the underlying act. (In fact, I believe conspiracy to commit a misdemeanor can be a felony!) The example a lawyer friend of mine came up with was: He says to two of us "Why don't we get together and monopolize sales of used cars in this state." One of us later goes to a used-car dealership and looks around. Theoretically, all three of us are guilty of conspiracy. Fortunately, conspiracy laws are used mainly as "add-ons" to provide bargaining chips for plea bargining in cases where crimes really have occurred. If they were abused, they might very well be tossed out as unconstitutional - though given the tenor of the times and today's court system, even that is hard to be sure of.

And you thought programming hard real-time systems was hairy!

Disclaimer: I'm not a lawyer, though I sometimes talk a bit like one. :-) The above is what I've gleaned from many discussions with lawyers over the years. (My wife's a lawyer. Many of her friends are lawyers. Many of MY friends are lawyers. A consulting contract I had not long ago was reviewed by no less than 5 lawyers on my side; had they all been charging me at their full rates, I would likely have gotten nothing out of the contract. Arrgh....) It is based on American law, and probably applies in more or less the same way under any system based on the Common Law - but who can tell.

-- Jerry

✓ Glass cockpits (A320, etc.)

Steven Philipson <stevenp@decpa.pa.dec.com> Thu, 7 Jun 90 19:49:48 PDT

In <u>RISKS 10.04</u> Henry Spencer (henry@zoo.toronto.edu) reports on an article in the April 30 issue of Aviation Week. In commenting on the article, Henry writes:

>(for example, NASA Ames, a major center of work on such things, >has no simulator representative of modern cockpits).

This is not quite what appeared in the article. Hart A. Langer (United Airlines VP flight operations) was reported to have said that "the center has no research simulator based on the glass cockpits that are in use today". [The quote is of Aviation Week paraphrasing Langer]. This is in fact true, however the Center does have a simulator on which the glass cockpits of today are based. This is the Advanced Concepts Flight Simulator (ACFS) at the Man-Vehicle Systems Research Facility (MVSRF) at NASA Ames.

This simulator had its origins about 10 years ago. It's display technology had definitely fallen behind the times, but was upgraded about a year ago with current technology computer graphics workstations which drive its displays. The displays are "representative of modern cockpits". My knowledge of this is first hand -- I designed and implemented the displays and software that drive the primary flight displays in the ACFS. They were intended to model prototype displays that Boeing was working on for the 747-400. NASA has now upgraded all of the displays and is actively performing human factors research on electronic flight instrumentation systems.

The general point of the article is correct however -- the technology is moving very fast, and it is difficult for the research institutions to keep up, let alone forge ahead. Thus new technologies are being fielded before their impact can be adequately assessed.

Steve Philipson

X Stonewalling with computers

Simon Turner <simon@robots.oxford.ac.uk> Fri, 8 Jun 90 18:47:18 BST

Back in March (shortly before the "Poll Tax" was introduced in England) I was having a little trouble persuading my local district council that I am a student, and as such need only pay 20 percent of the charge. During one of my many telephone calls to their offices, I was informed that their computer system (with all the data storage) was being upgraded, and I would therefore have to wait a long time while they tried to find my "real" file. I was given the distinct impression that it would be better if I rang back once the upgrade was finished, in a few weeks! Since this was only 4 weeks from the introduction of the Tax and I had no desire to pay 400 percent too much, I was quite prepared to wait and did so. My student status was eventually sorted out.

I don't believe for a second that my district council was trying anything clever, or that the situation was in any way other than as stated. However, it now seems to me that this would be an effective stalling measure for someone who wished to deny clients access to their records -- imagine a company in financial trouble stalling enquiries about outstanding orders with tales of an unavailable computer system (and hence unavailable records), while they quietly fled the country with the bank balance. This is something new (to me), and while it is not all *that* chilling in its implications, it's a thought.

Simon Turner, Robotics Research Group, University of Oxford, Dept. of Engineering Science, 19 Parks Road, Oxford OX1 3PJ, UK



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Tue, 12 Jun 1990 8:41:48 PDT

A woman identifying herself as Lisa Flowers used the secret code for Liz Taylor's answering service to set herself up as a cryptopublicist, returning telephone calls and giving out bogus interviews. She told reporters about a fabricated relationship with a 23-year Detroit man, Julian Lee Hobbs, and gave out false medical reports. The hoax included intercepting requests from UPI and AP for confirmation of earlier (phony) information, and providing confirmation! So much for "secret" codes. [Source: San Francisco Chronicle, 12 June 1990, p. 2]

EEC `IT Security Evaluation Criteria'

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 09 Jun 90 13:27 GMT+0100

This week, EEC sent the draft of the 'harmonized' Information Technology Security Criteria (ITSEC) to some people (I don't know the adress list) for comment. Based on the German 'Green Book', an expert group with French, German, Dutch and English contribution prepared a (greyly-white covered) booklet of 125 pages covering (after a short introduction: (1)scope) the functionality (2) and the assurance of correctness (3: 55 pages) as well as the assurance of effectiveness(4). The functionality chapter (2) refers, among others, to the Green Book's functionality classes F1..F5 (derived from Orange Book) and F6..F10 (adding availability and integrity of systems and networks to the well-known Orange Book functionality). The assurance part (3) elaborates the Green Books' quality Q0..Q7 into the more detailed `levels' E1..E6 (from 'inadequate assurance'=E0 equivalent to Orange Book 'D', towards E6 where correctness is formally proven (essentially A1, but not `beyond A1!); as in Orange Book and Green Book, each higher level encomprises the lower ones. For each level, specific features must be evaluated for the (4) 'phases' of the development process as well as for different `aspects' of the system and user documentation. Moreover, the effectiveness of the assured features is roughly described under aspects such as: suitability, binding of functionality, strength of mechanism, assessment of vulnerability (consstruction, operation), or ease of use.

EEC plans a conference in Brussels to happen on September 25-26, 1990. According to their letter, they welcome critical comments (if received by July 6th) which might be discussed in this conference.

Klaus Brunnstein University of Hamburg

PS: based on our analysis of the benefits and shortcomings of `Trusted Computer Evaluation Criteria' which we contributed to the IFIP SEC'90 conference, recently in Helsinki, I plan to analyse this new Criteria catalog in more detail. I would strongly appreciate any critical comments, as well on our paper on 'Risk Analysis of Trusted Computer Systems' (which I e-mail upon request) as well as on the above draft.

[The copy I have says that Der Bundesminister des Innern, Bonn, West Germany (Minister of the Interior) is der Herausgeber, so presumably copies can be obtained from there or from the other three governments. The ITSEC is a very deft merging of the earlier German criteria and the British claims language. PGN]

Ke: A 320 article in Aeronautique (Atkielski, <u>RISKS-10.05</u>)

Francois Felix INGRAND <felix@Al.sri.com>

8 Jun 90 22:46:13 GMT

- > Minor erratum: This article actually appears in the "Aeronautique"
- > section of the French science magazine "Science & Vie,"

In France, "Sciences et Vie" is considered as the "National Enquirer" of "Sciences"...

Most of their articles do not have the scientific seriousness you expect from a scientific publication.

Francois Felix INGRAND SRI International, AIC "Read my Lisp... No new syntax" (nil)

🗡 2600 magazine article

Arthur L. Rubin <arthur@pnet01.cts.com> Fri, 8 Jun 90 23:17:39 PDT

I posted the 2600 magazine excerpts on some local BBSs, and I have the following comment from a user and sysop:

What does the entire 911/Steve Jackson Games escapade tell us? Well, it's not all that new that the government (like most such things) requires careful watching, and I'm not too happy about how the last I'd heard, an agent had told SJ games they wouldn't get all of their hardware back, even though no charges had been filed (can you say legalized thievery boys and girls? I knew you could.)

But the main thing that moves me to write this missive is the indications from the published article that the authors, and thus quite likely also the party responsible for copying that document and circulating it still do not quite understand what the individual responsible did. Accordingly, and in the hopes that if this circulates widely enough he or she will see it, the following message:

OK - all you did was get into Bell South's computer system (mostly proving that their security sucks rocks) to prove what a hotshot hacker you were, then made a copy of something harmless to prove it. Sheer innocence; nothing to get upset about, right?

Bull****, my friend. Want to know what you did wrong? Well, for starters, you scared the US Government and pointed it in the direction of computer hobbyists. There are enough control freaks in the government casting wary eyes on free enterprises like BBS systems without you having to give them ammunition like that. Bad move, friend, bad move. You see, the fact that you didn't damage anything, and only took a file that would do no harm to Bell South OR the 911 system if it were spread all over the country is beside the point. What really counts is what you COULD have done. You know that you only took one file; Bell South only knows that one file from their system turned up all over the place. What else might have been taken from the same system, without their happening to see it? You know that you didn't damage their system (you THINK that you

didn't damage their system); all Bell South knows is that somebody got into the system to swipe that file, and could have done any number of much nastier things. Result - the entire computer you took that file from and its contents are compromised, and possibly anything else that was connected with that computer (we know it can be dialed into from another computer - that's how you got on, after all!) is also compromised. And all of it has now got to be checked. Even if it's just a batch of text files never used on the 911 system itself, they all have to be investigated for modifications or deletions. Heck - just bringing it down and reloading from backup from before you got in (if they KNOW when you got in) even if no new things were added since would take a lot of time. If this is the sort of thing that \$79,449 refered to I think they were underestimating.

You cost somebody a lot of time/money; you almost cost Steve Jackson Games their existance; you got several folks arrested for receiving stolen goods (in essence); you endangered a lot of bulletin boards and maybe even BBS nets in general. Please find some other way to prove how great you are, OK? --Crystalsword

Arthur L. Rubin, PO Box 9245, Brea, CA 92622 (work) (714)961-3771

Self-Replicating Bugs in Floppies

"Warren M. McLaughlin" &cLaughlin@DOCKMASTER.NCSC.MIL> Sat, 9 Jun 90 17:12 EDT

This is a personal report, eye-witnesses are available. On Thursday, 7 June 1990, at about 1500 hrs EDT, it was conclusively demonstrated that it is possible for self-replicating bugs to replicate themselves in floppies (5-1/4" DSDD) _outside_ of a computer!

There is a stash of scratch disks, in boxes, on top of a file cabinet next to my desk. Mostly, they are old backups awaiting degaussing and reformatting. At the back of the row of six or seven boxes, I found an open box of disks, with nine new, never-used disks. This minor treasure would have come in handy if I hadn't noticed visible evidence of the self-replication (and defecation) of the bugs, commonly known as "cockroaches".

A cursory examination, conducted after dropping the box in the trash bag, revealed at least five live beasties. Droppings/eggs everywhere in the box. I checked each disk envelope, and found spoor in all nine. Witnesses were drawn to the scene like flies... er, spectators. The was a certain amount of noise associated with the discovery, and the air in my cubicle is reported by some to have turned blue. This may be an exaggeration.

The droppings/eggs seemed large enough to have caused a head crash. I have enough bits loose in my PCs without adding more. I checked every other box, and found no evidence of infestation. Three of the boxes came from the same carton as the infested box.

I will not report the name of the manufacturer, as it does not seem important.

TechReps of several computer manufacturers have told me that "tower" style cases regularly attract cockroaches. They are thought to come in for warmth, or to eat the lacquer used on certain components. Incidentally, _real_ lacquer is the processed shells of the lac beetle, which is remarkably like a cockroach in appearance. (_cannabilistic self-replicating bugs?)

This may be yet another Risk of computing - or another Risk of working in an old five-sided building on the west side of the Potomac.

[Disclaimer: The views herein are mine of this fleeting moment, and neither represent my views upon considered reflection, nor those of the Department of the Navy, nor any component of the Department.]

- Mike

W. M. McLaughlin, Computer Security Coordinator, SECNAV/DONIRM(C2) Washington, DC 20350-1000

✓ Caller ID neither necessary nor sufficient to prevent crank calls

<ark@research.att.com> Sat, 9 Jun 90 13:20:02 EDT

The people who claim Caller ID is useful for preventing crank calls are somewhere between misguided and dishonest. Consider: do you *never* receive a call from someone you know from a phone number you don't recognize? Has you *never* had a friend call you from a pay phone? Of course not! So that means that a general strategy of refusing to answer calls from unknown sources will cut you off from some calls you would have wanted to receive.

Suppose, then, that you answer all calls. You are assured of getting a crank call from time to time. Why doesn't Caller ID avert that by making it known to the caller that you will identify the source?

It does, of course, but it's much more than you need for that purpose. For example, the following facility has been available in my calling area for some time: if after receiving a call I hang up, pick up the phone again, and dial *51, then a copy of the identity of the last call I received will be logged in the central office and I will be charged \$1.00. I can then call the police and tell them that I received a crank call that was recorded in the central office. They can find out who called and act appropriately.

So: even if I have Caller ID, I cannot avoid crank calls unless I also cut myself off from some legitimate calls. Once I have received a crank call, I can report the origin to the authorities even without Caller ID. How, then, is Caller ID useful for that purpose?

×

Peter da Silva <peter@ficc.ferranti.com> Sun Jun 10 10:34:19 1990 > As far as residential phone users are concerned, Caller ID is not much
 > better than receiving anonymous calls. [the message goes on to bring up "member of family at phone booth" considerations.]

I take it you have never been the target of telephone harrassment. I have. It's not a lot of fun, but unless it goes on for a long time it's just not possible to get the authorities to do anything about it. I have been called by my wife's ex-boyfriend (from his place of work!), by some bozo who threeway-called me to a third party, and by someone who calls and hangs up, we assume to call-wait my wife off a chat system (not knowing we have another line for the modem). In all of these cases caller-ID would be a deterrent, a channel of recourse, or a signal to ignore that call. Even when you know the harasser, there's not much you can do currently: when I called the ex back at work, he convinced his boss that *I* was harassing *him* (he'd called dozens of times... I'd called back once, then again when he hung up). If I'd had Caller- ID I could have just ignored calls from that number (the numbers handy to his place of work would have become quickly obvious).

In none of these cases was SWBell at all interested. In all of these cases Caller-ID would let me stop it in the bud. Calls from pay-phones just wouldn't have been possible for any of them (pay-phones don't have 3-way calling, and in the other two cases the opportunity wouldn't arise).

No system is perfect, but I'm not going to leave my door unlocked just because someone is capable of breaking a window. Making casual harassment less convenient is by itself a good thing.

Peter da Silva. +1 713 274 5180.

Ke: Risks of Laser Printouts (<u>RISKS-9.89</u>,91,92)

12 Jun 90 10:41:39 GMT

(Simson L. Garfinkel) writes:Not very surprising, considering that laser printers pump out gobs of ozone.

This is the first good news that I've heard!! With more and more laser printers we will be able to reverse the ozone destruction caused by all those CFCs floating around. :-) Can anyone quantify that figure: gobs? Ralph P. Sobek

Ke: egregious database -- risks of `voluntary' data submission

<janssen@parc.xerox.com> Fri, 8 Jun 90 16:19:21 PDT

in <u>RISKS DIGEST 10.07</u>, Edwin Wiles comments that the `egregious database' is less troublesome because of the voluntary nature of data submission. This ignores the risks of bureaucratization, in which the fact that one has not `voluntarily' submitted data to a database is held against one. (There is also the risk of inexperience, in that a student may not appreciate the consequences of putting personal data in a such a database, but this should always be considered.)

Bill

✓ Egregious Database ALREADY EXISTS

"William M. Bumgarner" <wb1j+@andrew.cmu.edu> Mon, 11 Jun 90 01:51:56 -0400 (EDT)

In the Columbia Public Schools, of Columbia, Missouri, such a system has been installed in the last few years-- it can keep track of basically _everything_ that can be recorded textually that has happened during a students K-12 academic career. Not only grades, but personality profiles, any comments by teachers, and just about anything that is even remotely associated with 'school' -- including incidences that don't appear on the 'permanent' record and incidences involving the police.

Apparently, the goal is to be able to track a student through the public education system and then store that data permanently ... and it is all at the fingertips (though, at many different security levels, of various random secrataries, counselors, etc.)...

b.bumgarner, NeXT Campus Consultant

KRE: Another egregious database (Wiles, <u>RISKS-10.07</u>)

Prof. L. P. Levine <levine@cvax.cs.uwm.edu> Sun, 10 Jun 90 12:55:23 CDT

In <u>Risks 10.07</u> Edwin Wiles, NetExpress, Inc., misses the point entirely. He seems pleased that the system is voluntary [...] But the next part of the quote is missing. Reading it from <u>Risks 10.05</u> we see:

<> The absence of criteria like punctuality might be noticed, however, <> just as vital information omitted from a resume would be, he adds.

and means that leaving out such information is itself an negative mark on the potential employee. I have students RIGHT NOW who are peeing in bottles (voluntarily) in order to get jobs. Of course they do not take drugs, of course they are doing it voluntarily, of course they want the job. They do it. Voluntary release of your civil rights is not protection. The argument that you have nothing to fear from this abuse of your rights if you are not guilty never washes. It is always just plain wrong. Nobody expects the Spanish Inquisition, but this is the way it begins.

Leonard P. Levine, Professor, Computer Science, U. of Wisconsin-Milwaukee Milwaukee, WI 53201 U.S.A.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Robert Nagler <nagler@olsen.UUCP> Fri, 15 Jun 90 10:47:46 +0200

Rust Imitator Flew Flowers to the Black Sea

By Elfie Siegl, Moscow - Reported in Tages Anzeiger, Zurich - 13Jun90

For the second time after Mathias Rust's landing on Red Square, a West German amateur pilot flew illegally into the Soviet Union with his private plane. As reported by the union newspaper "Trud", an unknown FRG citizen landed last Saturday [9Jun90] between 4 and 5pm at an airport in the Black Sea health resort, Batumi. He got out and distributed flowers, business cards, and leaflets which called for support of Gorbachov and of "perestroika". The Air Force Staff merely told Trud that many questions needed to be clarified. The press release of the Air Force Staff stated that such a small airplane "simply couldn't be noticed".

The pilot flew over Turkey towards the Soviet border south of Batumi, then under the radar control of the air force, and landed at the civilian airport in Batumi.

[I have three questions. Was this reported elsewhere? The Tages Anzeiger is not a rag. Secondly, the author states that this is the second time since Rust's famous flight. Who was the first imitator? Lastly, why was this not front page news? Is it to be assumed that any yokel can fly into Russia? Forgive my naivete.]

🗡 UK Hacker Goes To Jail

Robert E. Van Cleef <vancleef@fs01.nas.nasa.gov> Wed, 13 Jun 90 07:28:23 -0700

Posted: Sun, Jun 10, 19901:52 PM PDTMsg: SJJA-2888-9119From:RDAVISTo:MTynanCC:CWoodworth, RCarrSubj:UK Hacker Goes To Jail

Date: Fri, 08 Jun 90 09:10:12 +0100 From: Anthony Appleyard <PUM04@prime-a.central-services.umist.ac.uk> Subject: First jailed UK computer hacker

>From a UK newspaper called 'The Daily Telegraph', Friday 8 June 1990:-

['Mad Hacker' jailed for computer war]

A computer operator who called himself "The Mad Hacker" became the first in Britain to be jailed for the offence yesterday. Nicholas Whiteley, 21, of Enfield, north London, was sentenced to 4 months with a further 8 months suspended for criminally damaging computer disks and wreaking havoc on university systems. Whiteley, who, it was said, was driven by a desire top become Britain's top hacker, wept in the dock and held his hands to his face as he walked to the cells to begin his sentence.

Judge Geoffrey Rivlin, QC, described him as "very malicious and arrogant", and told him: "Anyone minded to behave in this way must be deterred from doing so.".

Whiteley declared war on computer experts, using a computer in his bedroom to swamp university computers with masses of useless material including threats and boasts about his brilliance. One said: "Don't mess with me because I am extremely nutty.".

He was found guilty last month of 4 charges of causing damage to magnetic

disks in mainframe computers at the universities of London, Bath, and Hull. The judge said some of the computers stored important and confidential data relating to medical and scientific research.

#.....

{A.Appleyard} (email: APPLEYARD@UK.AC.UMIST), Fri, 08 Jun 90 08:58:20 BST

🗡 Programmable parking meters

Kee Hinckley <nazgul@alphalpha.com> Fri, 15 Jun 90 01:53:27 EDT

According to the NYT Westwood Village and Reseda, CA are installing digital parking meters which can be reprogrammed (using an infrared beam) when the rates go up. Need I say more?

Ke: New computerized scoring system fails during Indy 500

Dave Horsfall <dave@stcns3.stc.oz.au> Tue, 12 Jun 90 12:29:21 est

This reminds me of the time a couple of weeks ago when I was taking part in a car rally, providing communications support. I was amused to hear some of the traffic being passed just after the race started, to do with two sets of fancy digital clocks that provided the elapsed times. It would appear that one of the clocks advanced itself by three minutes, as a result of nearby UHF CB activity from the race marshalls. It did not seem possible (or perhaps legal) to alter the errant clock, so from there on the time had to be adjusted manually before being reported. Since the average lap time was about one minute such a failure was obvious, but had the course been much longer then errors could easily have crept in.

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

Ke: Caller ID for dealing with anonymous callers (<u>RISKS-10.08</u>)

Marc Shannon <YNFUL@DRYCAS.CLUB.CC.CMU.EDU> Tue, 12 Jun 90 21:39 EST

From what I understand, Caller ID *cannot* be used to report crank phone calls. It is simply provided (in some areas - Pennsylvania's legislature has ruled that Caller ID is an invasion of privacy) as a convenience.

In order to legally report the phone number of a crank call without prior tracing arrangements with Bell's Nuisance Call Group, one needs to use the Call Trace function which reports the caller's phone number to Bell while keeping the number secure from the call's recipient.

The only thing I couldn't understand is that it seems that the ability to "Call

Trace" is an optional service (costing $^{1.50}$ /month). I would imagine that it would be in the public's better interest to make it available to anyone since one usually cannot anticipate when such a call might be made.

(I'd love to report the numbers of these calls that I get telling me that I need to call 976-xxxx RIGHT NOW. I definitely consider these to be a nuisance!)

--Marc

Ke: Liz Taylor and ``secret codes'' (<u>RISKS-10.08</u>)

Randal Schwartz <merlyn@iwarp.intel.com> Tue, 12 Jun 90 12:17:37 PDT

My answering service told its customers in a recent "fact sheet" that the software they run is used at many (over 200?) locations around the US.

I pick up my messages by calling a "message-number" and dialing a five digit code. The first four digits are nothing more than my account number (assigned sequentially beginning at 0000), and the last digit is whatever it takes to make the number a multiple of nine (casting out nines)!

How simple. It'd be trivial for me to read anyone's messages. In fact, since the mapping from DID number to the account number is fairly easily determined from a few tries (293-[78]XYZ maps into "account" [12]XYZ, for example), I could scan the phone book for rented numbers from this answering service, and scam on just about anyone I felt like.

Security. Ha. If this is the same software that's running on hundreds of sites around the country, lots of answering services are very vulnerable.

Just another person that doesn't always answer the phone,

Randal L. Schwartz, Stonehenge Consulting Services (503)777-0095

EEC ITSEC adresses

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 14 Jun 90 12:44 GMT+0100

As the EEC IT SEcurity Criteria have been constructed from groups in 4 EEC member countries, the paper can be ordered from any of the following adresses:

for France: Service Central de la Security des Systemes d'Information Division Information et Systemes 18 Rue du Docteur Zamenhof F-92131 Issy les Moulineaux (apology for missing accents)

for Germany: Zentralstelle fuer die Sicherheit der Informationstechnik (ZSI)

Am Nippenkreuz 19 D 5300 Bonn 2

for The Netherlands: Netherlands National Comsec Agency Bezuidenhoutseweg 67 P.O. Box 20061 NL 2500 EB The Hague

for United Kingdom:

Head of UK CLEF Scheme Certification Body CESG Room 2/0805 Fiddlers Green Lane Cheltenham GLOS GL52 5AJ

For those interested in the Green book: you may receive a copy (English or German) from ZSI (=German Information Security Agency, GISA), adress above; essential parts of Green Book (esp. the functional classes F1-F5,F6-F10) are also in EEC ITSEC' annex A, while the 'quality classes' Q0-Q7 have been adapted and partly enhanced with ideas from the other countries' criteria catalogs.

Klaus Brunnstein University of Hamburg

🗡 I APOLOGIZE

Danny Cohen <OHEN@venera.isi.edu> Fri 15 Jun 90 13:32:51-PDT

In <u>RISKS-10.05</u> I expressed some "minority opinion" about the article on A320 in Aeronautique, April 1990 (<u>RISKS-10.02</u>). The article that was written by Mr. Bertrand Bonneau and translated to English by Pete Mellor.

While taking issue with the original article, I tried to compliment the translation. In trying to do that I made a terrible mistake by refering to Bertrand Bonneau as the "the translator to English". This mistake offended the Pete Mellor to no end, as he expressed in RISK-10.06: "If this is a joke about the translation, it's a bit too subtle for me!"

I APOLOGIZE FOR THIS MISTAKE !

[An explanation (not an excuse): After composing my message about the article I looked for the translator's name and misread the line: "Translation of article by Bertrand Bonneau" as if the translation, not article, was by Bertrand Bonneau.

I read it as: "Translation (of article) by Bertrand Bonneau" in stead of : "Translation of (article by Bertrand Bonneau)".

RISKS readers are kindly asked not to submit contributions about "Risks in Using Languages with Ambiguous Syntax" and not to recommend using LISP as the ultimate solution. In later issues of RISKS several contribution expressed strong disagreements with what I submitted.

One of the key points made by them that in this case (unlike many others) as expressed in:

<> "The pilot and copilot survived the Mulhouse crash, and immediately <> made statements implicating delays in engine acceleration (Times 27th <> June 1988)".

Another point is the rush to judgment motivated by the desire of the French airlines/Industry/Government/etc., not to ground the aircraft. This was expressed in:

<> "...the day after the accident, the DGAC announced a preliminary <> conclusion that the pilots, and not the aircraft, were to blame for <> the disaster. According to the French press, details of the flight <> records were given to Aerospatiale, which announced that it had <> confirmation that the aircraft was not at fault in the crash. Several <> days later, the DGAC exonerated the mechanical performance of the <> Airbus. The head of the DGAC, Daniel Tenenbaum, said that if this had <> not been the case, it would have been necessary to ground the A320 <> for tests."

<> (And we couldn't have that, now, could we? :-)

<> [In fairness, I should add that I have spoken to a number of people <> in the CAA and elsewhere who know a lot about flight certification <> and about the Mulhouse accident in particular, who have assured me <> that it *was* pilot error, but, as always, confidentiality prevented <> them from saying *how* they knew that.]

Facts (that took very little time to find after the accident) included that the pilots flew too slow and too low (e.g., as I remember it the pilots submitted plans for 100' and flew at 35'), that due to the high pitch angle the pilots didn't see early enough the terrain into which they flew, and that the pilot disconnected some of the safety systems (some of RISKS readers complained later that it is not safe for an aircraft system to allow manual override and disconnection -- [this was probably submitted by non-pilots]). All of that was confirmed by the FDR. [By the way, it shouldn't take more than just a few hours to read the FDR.]

The surviving pilots (from the hospital) complained that it took too long for the engines to regain their power. Many consider the pilots' statement to be too self-serving (what a surprise!). It was the opinion of many (including not only the FAA/NTSB-like organizations but many people even in competing aircraft engine companies) that this delay was well within the normal response of such an engine.

Based on the above the aircraft was cleared ("un-grounded").

History didn't prove this decision to be wrong. Danny P.S., About the timeliness of Aircraft Accident investigation reports: The NTSB report about the UAL DC-10 crash at Des Moines, Iowa, on July-19-89, is not out yet (as of June-15-90).
Image: A state of the st



<junger@cwru.cwru.edu> 16 Jun 90 14:43:00 EST

Nearly twenty years ago a full text electronic database of legal opinions named OBAR was released upon the world. Each word (except for common ones like `the' or 'is') in each opinion included in the database was placed in an inverse file with a pointer to where that word appeared in the database. This allowed for rapid on-line boolean searching for cases containing certain specified terms. Thus a search for "cat and (dog or hound)" would produce a list of all opinions in the database in which the word `cat' appeared together with the word `dog' or the word `hound' (or both). This OBAR system has grown over the years into the Lexis system (including the Nexis collection of newspaper and magazine articles) run by Mead Data Central which is the largest fulltext documentary database in the world.

I have always assumed that the two major risks associated with using this system are: 1.) the fact that a document might not have been entered into the database or, if it was entered, that it might have been entered incorrectly and 2.) the tendency of a user who found a bunch of documents (that seem to be what is wanted) to assume that _all_ the relevant documents had been found. Type II errors--documents found that are not what one wants, i.e., false positives--are easy to spot on Lexis and similar systems, but type I errors--documents that should have been found, but weren't--simply don't show up in a search.

On last Wednesday, however, I realized that I had been rather naive. On that day I ran a bunch of searches in the United States Supreme Court Library on Lexis each of which was in the form: "ENTITLEMENT and DATE(BEF 1/1/19x0) and DATE(AFT 12/31/19y0)" where y=x+1. Each of these searches should have produced a list of all the opinions of the United States Supreme Court during a particular decade that contained the word `entitlement'. (Actually, since the date field in the Lexis database contains the date of argument as well as the date of decision, there would be some overlapping of the cases in the various lists, but this is easily adjusted for.) But that is not what I got. Instead I got identical lists for the 1940's and 1950's and both of these lists contained the same documents--which were, to make thing's worse, opinions handed down in the 1980's.

I reported this to one of our research librarians who tried to make the same searches and got the same results. She then phoned Lexis's customer representatives who in turn made the same searches and got the same results. The customer representatives thanked our librarian for brining this interesting situation to their attention and promised to phone her back.

And they did phone her back quite promptly. It seems that Lexis had installed new searching software back in May sometime and that this new software has a bug in it when doing date delimited searches. They hope that it will be fixed in a couple of weeks.

I suppose I was lulled into a false sense of complacency because I have used this system for over 20 years and because its boolean searching capabilities have always seemed to me too primitive to be buggy. But now I wonder how many lawsuits have been won or lost--or how many law review articles have contained worthless data--because of defects in the searching software rather than the user's searching strategy.

This particular example involved Lexis, but now I worry also about its competitor Westlaw and about all the other textual databases such as Dialog. Have similar problems ever arisen with the many on-line scientific databases?

Peter D. Junger--Case Western Reserve University Law School--Cleveland, OH

🗡 computer security problems in Malaysia

<smb@ulysses.att.com> Mon, 18 Jun 90 03:58:59 EDT

According to the AP, a newspaper in Malaysia reports that a bank executive ``cracked'' the bank's computer security system, and transferred money from some clients' accounts to his own. The loss was discovered by an audit, and he had made himself conspicuous by buying several expensive new cars. The executive allegedly looted \$1.5 million.

--Steve Bellovin

🗡 canopus.stanford.edu goes nova

Joe Dellinger <joe@hanauma.stanford.edu> Mon, 18 Jun 90 03:24:17 PDT

Saturday night someone exiting an office 60 feet away from mine discovered the hallway full of acrid fumes; they ran choking down the stairs to get away. They called Stanford Health and Safety, who came with air-sampling meters and identified my office as the source. By this time the whole building reeked; people were getting headaches from the fumes. The Health and Safety people thought the fumes smelled like bromoform, a common chemical used in analyzing rock samples that we've had problems with before when a fumehood malfunctioned. But there are no fume hoods on my floor, which perplexed them. (No windows either, even though we're on the 4th floor; Stanford's red tile roofs take precedence over student offices having windows. The extremely poor air circulation on our floor is a continual cause of complaints from the students here.)

Since it was my office I was called at home; they were trying to puzzle out how dangerous chemicals could be getting into my office. Fortunately we were able to point them on the right track immediately: the source of the toxic fumes was my Color Sun 3-110 monitor! How were we so sure? Because the same thing happened a year previously to a similar Sun monitor on our floor! That time it wasn't on a weekend, so the building circulation was in higher gear, and the building happened to be empty so when people arrived most of the fumes had dispersed. Still, last time that office was unuseable for a couple of days. This time, a day after the event my office still gives me a headache within a minute or two of entering, and makes my eyes sting. The Health and Safety people carted my Sun monitor away in a sealed plastic bag used for carrying "hazardous material"!

Stanford Health and Safety was quite concerned about this incident. There are a LOT of Sun workstations around here. They've never heard of this happening before, and want to find out more about this "risk of workstations". So:

1) Has anybody else out there had this happen? Since we only have

about 15 Suns, and it's happened to two of them now, it seems it must be pretty common. But if that's true why hasn't Health and Safety heard of this happening at Stanford before? Is it just because we have such bad ventilation here? Perhaps the computer scientist types who have most of the workstations on campus never work with dangerous chemicals, so they always just open the windows and forget about it?

2) What IS that nasty chemical? Health and Safety take anything that gives near instant eye burn and headaches VERY seriously. Will I have bury all my books in a toxic waste dump?

Too bad, and I was just learning to type slowly enough so that my Sun keyboard wouldn't go "click" and eat a random character or two every other sentence...

Ke: UK Hacker Goes To Jail (<u>RISKS-10.09</u>)

Pete Mellor <pm@cs.city.ac.uk> Mon, 18 Jun 90 13:56:07 PDT

With regard to the imprisonment of Nicholas Whiteley for 4 months, and the Computer Misuse Bill currently going through parliament, it is worth noting:

- Whiteley was convicted on four charges of malicious damage to property.
 This offence has nothing specifically to do with computers: you can be charged with the same thing for breaking down the fence of the local swimming pool (as a colleague of a friend of mine found to his cost after he decided to go for a midnight swim after a party).
- The provisions contained in the Computer Misuse Bill would not have assisted in his detection or conviction. It is possible that the charge sheet could have been made longer: separate charges of i) unauthorised access,
 ii) unauthorised access in furtherance of a more serious crime (i.e. damage), and iii) the damage itself. Whether this would have attracted a more severe sentence is doubtful. The prosecution claimed that the cost of the damage was 25K pounds sterling. If that amount was believed by the court, and it still led to four months only, it is difficult to believe that the addition of the ancillary charges would have caused the judge to take a more serious view of the case.
- It is also difficult to see how the amendment proposed by Emma Nicholson, to increase police powers of telephone surveillance, would have assisted in his capture.

Far from indicating the need for new anti-hacking laws with tougher sentences and more loosely-defined offences, this case goes to show that where hackers actually do damage, the existing laws are adequate, and that the main problem is, and will remain, that of catching them.

Pete Mellor

Air India votes no confidence in A320

Andrew Klossner <andrew@frip.wv.tek.com> Mon, 18 Jun 90 08:12:49 PDT

Air India ran an ad in the Wall Street Journal: they're trying to sell all their purchased A320s and sublease their leased A320s.

-=- Andrew Klossner (uunet!tektronix!frip.WV.TEK!andrew) [UUCP]

A320 near-disaster (from <u>RISKS 1-2</u>-34)

Robert Dorsett <rdd@ccwf.cc.utexas.edu> 18 Jun 90 19:29:31 GMT

This is from the French science biweekly "Mon Dieu" Translated and reprinted without permission:

"TOULOUSE,

French aviation authorities here admitted to a near-disaster which occured about a month ago aboard an Airbus A320 jetliner. The controversial aircraft with its 'fly-by-wire' flight controls has been the subject of intense controversy since its introduction. The manufacturer, a consortium of European interests, has steadfastly maintained the aircraft's inherent safety over other aircraft, largely as a result of the computerized controls which limit inputs from the pilots to ensure they are always compatible with the current aerodynamic state of the plane. Pilots and other pundits have argued that these same safeguards can severely limit the crew's options in emergency conditions. Additionally, they argue that the increased faith placed in the on-board computers leads to crew complacency and inattentiveness.

"The incident in question took place while the aircraft, a British Airways plane, was at cruise between New York and Fairbanks. The co-pilot was apparently entering new navigational data into the craft's INS (Inertial Navigation System) when he misstyped a code. The INS came back with 'Invalid PIN number selected' and returned the craft's weight and balance data to the astonished crew. 'We tried several more times," exclaimed Reginald Dwight, the Captain, 'and every time it was the same thing. On the third try it said "Access violation, contact your credit institution if you believe there is an error." At that point all the plane's controls froze and it refused to respond to our commands. We didn't know what to do, so we got on the radio."

:British Airway's mechanics were equally dumbfounded and decided to call French mechanics. France's Aerospatial is the prime contractor for the aircraft. 'The French were totally rude to us,' stated an unnamed BA mechanic. 'They stated the problem was our fault and that "the pasty little Englishman probably had too many meat pies and Guiness".' 'It wasn't until we told them that Jerry Lewis was aboard the flight that they became concerned.'

"French mechanics traced the problem to the ATM-6000 INS computer, which was a modified version of a computer used in the United States for bank transactions. 'Essentially, the INS decided that the co-pilot was trying to rip-off someone and locked the controls.' French authorities then assured the English crew that the system would automatically remove the restrictions at the start of the next banking day. 'We told them that we would be in the sea by then!' exclaimed the frustrated copilot, Nigel Whitworth.

"A French team, headed by Bertrand Swatboutie, determined that manual control of the plane could be re-established if a crewmember went back to the tailcone and operated the elevators manually. The rudder is linked by backup cables to the cockpit and with the crewmember operating the elevator they determined they would have enough control. 'There is nothing wrong with ze plane,' exclaimed Swatboutie, 'that a little pinch in the rear will not cure. Just like a woman. If these English souffres knew anything about women, they would never have had to call us in the first place.'

"The plane was able to safely land at Denver's Stapelton airport, where the craft was repaired and all crewmember's credit histories reviewed."

DISCLAIMER: I used to live in France and some of my best friends are... never mind.

Gregory R. Travis Indiana University, Bloomington IN 47405 greg@cica.cica.indiana.edu Center for Innovative Computer Applications N5457E, C-172

RISKS of computers in medical offices

Arthur L. Rubin <arthur@pnet01.cts.com> Mon, 18 Jun 90 18:35:00 PDT

Recently, my wife was taken to a local hospital (which shall remain nameless) for uncontrolled bleeding after a cut in the kitchen. (She seems to be fine now, but the cut required 3 stiTches.) While we were waiting to see the doctor on duty, we saw a man wearing a stethoscope coming in the admitting room to try to fix the printer used to print admission and insurance forms. We later found out that he was the doctor seeing patients that day for the emergency room. Another patient waiting had a possible concussion.

The risks are obvious.

Arthur L. Rubin, PO Box 9245, Brea, CA 92622

More Space Telescope Problems

Karl Lehenbauer <karl@sugar.hackercorp.com> 19 Jun 90 03:09:36 CDT (Tue)

The June 18th issue of Aviation Week and Space Technology has a half-page article on two problems the Hubble Space Telescope has been having.

One problem is that some RAM used by the fine guidance system is being scrambled when the telescope passes through the South Atlantic Anomaly, a region representing a "dip" in the Van Allen Belts that has been known to be hazardous to spacecraft electronics for decades. This happens for a ten minute period during every 98-minute orbit. The NASA deputy project manager of the HST, Jean Olivier, said that they had evaluated the radiation effects very carefully, but that they had apparently miscalculated.

The data in the RAM is supplied, according to the article, by the telescope's Rockwell Autonetics DF-224 general purpose computer. The magnetic core memory used by the Rockwell computer is not considered to be susceptible to disruption by radiation. Olivier said that the Rockwell computer can be programmed to refresh the RAM ten times a second, with the result being that a completely new set of parameters in the fine guidance sensor electronics would be calculated every five seconds, thereby eliminating the problem.

The second problem is with the telescope's solar arrays. Analyses done in Europe and the United States sugest that the poles that hold the solar arrays in place, called bistems, bow under a 50F degree temperature gradient, causing the ends of the arrays to move about ten inches, resulting in their oscillating for up to six minutes. Olivier said that the solution is to program the spacecraft's magnetic torquers to apply counteracting forces.

Invisibly long lines

<whb@hoh-2.att.com> Tue, 19 Jun 90 08:53:19 EDT

I don't know if this counts as a Risk or not, except for programmers (such as myself) who occasionally fall into the trap of "Nobody'll ever need a line longer than N characters."

In RISKS-FORUM Digest Volume 10 : Issue 02, the following paragraph appears:

--- Begin included paragraph ---

Although what have come to be called the "Chirac flight" and the "Habsheim affair" are the two facts most known to the public, the first year of operation of the A320 has been marked by numerous incidents which have directly called into question certain systems on the aeroplane. Often badly received by the first crews qualified on this aircraft, and sometimes vigorously denied by the technical directors of the launching companies, these incidents lead one to ask if the manufacturers and the certification authorities have not proceeded a little too quickly.

--- End included paragraph ---

Those of us looking at that on an 80-column screen see nothing wrong, but I chanced to be using a wider screen and saw that the line which begins "technical directors" actually wraps around to the next on-screen line and ends with "not proceeded a" - a total of 155 chars + newline.

No, my editor of choice had no trouble with it, but I can think of several programs which do text handling which would.

Wilson H. Bent, Jr. ... att!hoh-2!whb (whb@hoh-2.ATT.COM) AT&T - Bell Laboratories (201) 888-7129

Water problems

Gene Spafford <spaf@cs.purdue.edu> 18 Jun 90 17:22:51 GMT

Story 1.

I don't have a newspaper citation for this story -- I heard it on the phone last night while talking with a friend in Atlanta.

It appears that in north Fulton County, Atlanta, a water main broke inside one of the pumping stations. The resulting flood damaged 4 of the main pumps and they had to be taken offline. The area was without normal water pressure for a few days, and some places were completely without water.

The Risk? Well, the computer center where they have the machines running the Avail ATM network for Atlanta was in that area. And they evidently depend on the public water system for cooling (either the building or the machines themselves -- it wasn't clear to my friend from the news reports). The center had to be shut down until normal water service was restored, thus "un-Availing" ATM customers throughout the Atlanta area.

Story 2.

At 4am on the 7th of this month, a 14" water main broke in one of the service tunnels here on campus. Unfortunately, it broke in a tunnel connected to the campus computing center (conveniently located in the basement of one of the buildings). What happened next was nasty. In the words of George Goble of our ECN staff:

> I heard there was eventually 2-3' of water down there, about 500,000 Gal,
> more than the city swimming pool. Gives a new meaning to "floating point
> overflow", and "source pool", etc. Water came in so fast, it went up at
> 1-2" per min, and the mech equipment room (with 100HP motors for air
> handling, etc) became submerged while in operation.. no more motors!
> 480V running around everywhere, 12KV in the (flooded) tunnels!

> There were reports of Macintoshes and PC's starting to submerge, and
> water blowing out the fans, and fire/smoke coming out the power supplies.
> Floor tiles were floating down the hallway, until they bumped into
> something, releasing trapped air, and sank. There was a pallet or
> two of water softener salt stored in the basement also, I heard some
> PC's had only the plastic remaining, as the salt/corrision had eaten

> away the metal. Early on, someone said they saw an elevator which
> had stopped at the basement, go up one floor, open its doors, and
> 3' of water poured out on ground floor.

The service tunnels out of that building were also flooded, and helped carry the water into the basements of nearby buildings. That's good, in one sense, or the water would have gotten much deeper in the computing center.

Then, to make the whole situation even better, the folks who were pumping stuff out used gasoline powered pumps that filled the entire Math/Science building with carbon monoxide leading the police to cordon off the building and prevent anyone from getting to their offices. This included the Math & Stat departments, the math sciences library, and the Dean and his staff.

Amazingly enough, some of the networks and machines were up and in normal operation by the end of the weekend. This was good, because the networks coming into campus are routed through that complex.

Luckily, our CS computer room is on the 2nd floor of another building, and our ECN computer center is across campus. Other sites, similarly isolated were also unscathed.

Morals:

1. Basements are not the best place to keep your computers

2. Depending on outside water (or lack thereof) to keep your machines running can be a mistake.

3. If you do pipeline processing, be sure to check for overflow!

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



Search RISKS using swish-e

Report problems with the web pages to the maintainer



M The Risks of Reading RISKS (Re: Travis, <u>RISKS-10.10</u>)

<kgd@informatics.rutherford.ac.uk> Wed, 20 Jun 90 09:41:07 BST

If RISKS editorial policy is to publish hoaxes, jokes and elaborate fictitious accounts of non-events, at any time of the year *without* explicit warning, then its purpose will have been undermined.

The article by Gregory Travis of Indiana "University" about the A320 may have been jolly good humourous nonsence, but it was presented as a genuine RISK. There are other news groups and mailing lists for jokes. RISKS is for RISKS!

Which introduces another abuse of information technology: when is an article in RISKS a real RISK? How many other published articles have

been mere hoaxes? How are we to know?

I think an explanation is required.

Keith Dancey, Rutherford Appleton Laboratory, Chilton, Didcot, UK

Ke: The Risks of Reading RISKS

RISKS Forum <risks@csl.sri.com> Wed, 20 Jun 1990 7:52:02 PDT

I am very sorry for any confusion. I inadvertently deleted the line that said that the message was from rec.humor. (I'm glad only a few of you took it seriously, although I am also sorry to besmirch my own efforts to provide incisive and consistent moderation.) Too bad that the tale was not sufficiently outrageous that it could not have been true!

I was editing remotely under tight time pressures. I also omitted from the Contents of the issue Steve Bellovin's item on computer security problems in Malaysia, also attributable to the same editing difficulties. Editing through an imperfect terminal emulator can be quite risky.

"Artificial Life" out of control

Nathaniel Borenstein <nsb@thumper.bellcore.com> Thu, 21 Jun 90 08:34:25 -0400 (EDT)

The latest issue of the Whole Earth Review has an article ("Perpetual Novelty") about the growing "artificial life" movement, which works to create computer simulations of artificial beings, with rather far-fetched and grandiose long-term goals. I was particularly struck by the discussion of the idea that some of these people have to release lots of relatively dumb robots and simply let them evolve. Talking about one researcher's goals, the article says:

He wants to flood the world (and beyond) with inexpensive, small, ubiquitous thinking things. He's been making robots that weigh less than 10 pounds. The six-legged walker weighs only 3.6 pounds. It's constructed of model-car parts. In three years, he'd like to have a 1mm (pencil tip-size) robot. He has plans to invade the moon with a fleet of shoe-box-size robots that can be launched from throw-away rockets. It's the ant strategy: send an army of dispensable, limited agents coordinated on a task, and set them loose. Some will die, most will work, something will get done. In the time it takes to argue about one big sucker, he can have his invasion built and delivered. The motto: "Fast, Cheap, and Out of Control."

I think that about says it all. The risks should be obvious, at least to the people who read RISKS.

Nathaniel S. Borenstein, Member of Technical Staff, Bellcore, Morristown, NJ

✓ Update on Alcor/email case (at last)

<hkhenson@cup.portal.com> Thu, 21-Jun-90 01:40:38 PDT

Update on the progress in the Alcor/email case as of June, 1990 (originally reported in comp.risks)

by H. Keith Henson

A suit under section 2707 of U.S.C. title 18 (the Electronic Communications Privacy Act) against a number of individuals in the Riverside, California Coroner's office, the District Attorney's office, and the Riverside police department was filed Jan. 11, 1990, one day short of the statutory limit. There were 15 plaintiffs out of roughly 50 people who had email on the Alcor system. For those of you who are not familiar with the case, the coroner removed a number of computers from Alcor in connection with an investigation into the cryonic suspension of Dora Kent in December of 1987.

The defendants moved in March for a dismissal of the case, arguing that 1) the warrant for the computer was enough to take any email found within it, and 2) that even if the defendants had made "technical" errors in confiscating the email, they should be protected because they acted in "good faith."

Our lawyer opposed the motion, arguing that the warrant originally used was itself defective, even for taking the computers. This is something Alcor had never done, because (I think) people can only object to a warrant after charges have been filed, and for all the accusations the coroner and DA made in the press (which included murder, drugs, theft, and building code violations), no charges have been filed in this case in the last two and a half years.

The federal judge assigned to the case denied the motion after hearing oral arguments in May. Based on the comments of the judge from the bench, it seems that he agrees that the plaintiffs have a case, namely that taking email requires a warrant for the email, or the persons doing so will face at least civil liability.

So far the legal bill stands at over \$10,000. Suggestions as to organizations or individuals who might be interested in helping foot the bills would be welcome. (Donations would be returnable if we won the case and the county has to pay our legal bills as required in section 2707.)

The text of the legal filings (40k, three files) have been posted to CuD. If you can't get CuD, they are available by email from hkhenson@cup.portal.com

"Unbreakable Math Code Finally Broken"

<jbr@cblph.att.com> 21 Jun 1990 7:50 EDT [The following article appeared in the 06/20 Columbus (Ohio) Post Dispatch, credited to the Washington Post.]

Two mathematicians, working with hundreds of colleagues, announced yesterday that they had broken a code viewed by many cryptographers and security experts as virtually impenetrable. The feat, in which the mathematicians factored one of the world's ``most wanted'' numbers, means that many security-minded organizations will need to change their cryptographic systems to prevent security breaches.

"In the long run, mathematical breakthroughs like this will make everyone more cautious about how far one must go to keep a message private," said Arjen Lenstra of Bellcore, the research arm of the major regional telephone companies. Lenstra, with Mark Manasse of Digitial Machine Corp., successfully factored a 155-digit number, a feat many mathematicians had believed to be prohibitively difficult.

Cryptographic systems are used to encode messages and data before they are sent among banks, corporations, governments, the military -- anyone wishing to avoid having computerized mail perused by outsiders. The sender encodes messages using a many-digit number that would be difficult or impossible to factor. [...] Only someone who knows the factors of the large number can decode the message. Until now, it was thought virtually impossible to factor a number 155 digits long, and many cryptographic systems used numbers that long to encode their messages.

The work of Lenstra and Manasse, and hundreds of mathematicians who plugged the Bellcore program into their computers at night to solve additional parts of the problem, changes the game. Lenstra now says security-minded users must now find numbers greater than 200 digits to feel safe. Lenstra and Manasse, chewing up the equivalent of 275 years of computer time, found that the 155-digit number could be factored by a 7-digit number, a 49-digit number, and a 99-digit number.

[This certainly points up the risks of supercomputers and high-precision math, not to mention the risks of the press reporting on computer-related topics. :-) -- jab]

Joe Brownlee, Analysts International Corp. @ AT&T Network Systems 471 E Broad St, Suite 1610, Columbus, Ohio 43215 (614) 860-7461

A (rather old) risk of new technology

Clive Feather <clive@x.co.uk> Mon, 25 Jun 90 17:12:29 bst

>From the Cambridge Weekly News (a free newspaper) 31 May 1990.

"... [in 1927] by the first traffic lights [in Cambridge] at the bottom of Castle Hill. These were supposed to replace the policeman usually stationed there on point duty but, according to some sources, actually meant that two police were needed - one to explain the system to befuddled motorists and the other to hold back the crowds of onlookers enchanted by the pretty changing lights."

[BTW, that's Cambridge, Cambridgeshire, not Cambridge, Massachusetts]

Clive D.W. Feather, IXI Limited , 72-74 Burleigh St., Cambridge CB1 1OJ UK

Kisk submitting papers by e-mail!

&onathan.Bowen@prg.oxford.ac.uk> Wed, 20 Jun 90 16:11:28 BST

An electronic mail system should not tamper with the contents of the messages which it conveys. However, when sending messages via Unix electronic mail, any line starting with "From" in the body of the message has a ">" prepended to it to avoid the line being confused with a "From" line in the header which is used to delimit messages in a mail box file. However, such lines are not that uncommon in text. Source text for publication is now more and more routinely being sent via e-mail, and any changes in the message could easily end up being printed since it is often assumed that the text has already been proof-read.

As an example of this, see the paper "Some comments on the assumption-commitment framework for compositional verification of distributed programs" by Paritosh Pandya, in "Stepwise Refinement of Distributed Systems", Springer-Verlag, Lecture Notes in Computer Science no 430, pp622-640. On pages 626, 630 and 636 three paragraphs start with a "From" and have an upside-down "?" just beforehand. (This is what the LaTeX document preparation system transforms ">" to in the standard font.) [...]

Jonathan Bowen, Programming Research Group, Oxford Univeristy.

Ke: The Hubble Telescope (<u>RISKS-10.10</u>)

Tony Ozrelic <tonyo@sagerat.cna.tek.com> Tue, 19 Jun 90 15:58:09 PDT

...One problem is that some RAM used by the fine guidance system is being scrambled when the telescope passes through the South Atlantic Anomaly, a region representing a "dip" in the Van Allen Belts that has been known to be hazardous to spacecraft electronics for decades...

This Anomaly wouldn't have to do with the Bermuda Triangle, would it? :)

tony o.

Ke: DEC RA90 disk failures: correction/update

David Keppel <pardo@cs.washington.edu> 21 Jun 90 16:14:23 GMT Recently I posted an article about a DEC RA90 disk failure that we had in February, and said that DEC had not notified customers of the problem. I have since found out from our lab staff that DEC *did* notify customers. It looks like I screwed up, not DEC.

Prior to our failures, and several others that occurred at about the same time, DEC believed that, of the drives with serial numbers in the ``possibly affected'' range, either they failed when brand new, or they were ``safe''. Ours were among the first ``midlife failures''. In response, I understand that DEC replaced all RA90s with serial numbers in the ``possibly affected'' range, even though only 2% of these drives ever experienced failures.

So DEC 1, me zero.

Also, my original posting had deserved a followup anyway, but doubly so in this case: I had included a disclaimer in my original message, but the RISKS moderator clipped it off when he compiled the digest. When I saw that, I considered posting a RISKS article about the risk of losing disclaimers, but decided against the extra traffic. Wrong again....

{rutgers,cornell,ucsd,ubc-cs,tektronix}!uw-beaver!june!pardo

[PLEASE NOTE THAT THE PAST FEW ISSUES HAVE HAD A GENERIC MASTHEAD DISCLAIMER. I GENERALLY TRIM ALL SORTS OF TRAILING POETRY, SCATOLOGY, HUMOROUS DISCLAIMERS, LATITUDE AND LONGITUDE, HOME PHONES, etc. IF YOU HAVE A REALLY IMPORTANT DISCLAIMER THAT YOU FEEL SHOULD NOT BE SO DELETED, PLEASE LET ME KNOW. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



747-400 computer problems cause excess departure delays

Jon Jacky, University of Washington <ON@GAFFER.RAD.WASHINGTON.EDU> Mon, 25 Jun 1990 17:33:41 PDT

Here are excerpts from THE SEATTLE POST INTELLIGENCER, March 22, 1990, p. B7:

BOEING TASK FORCE TACKLES PROBLEMS WITH THE 747-400 by Bill Richards

After a year on the job, Boeing's newest jumbo jet, the 747-400, has piled up more mechanical delays at the departure gate than any of the company's jetliners since the first 747 went into service 20 years ago.

Boeing officials said yesterday they knew about problems with two especially troublesome pieces of equipment --- a computerized power unit used to start the plane's engines and a computer that spots maintenance problems --- but decided to sell the jumbos anyway. ...

(Boeing official Robert A.) Davis said the problem with the 400's engine power unit was caused by unusual sensitivity in the unit's digital monitoring system. If the plane switches from ground power to auxilliary power to engine power in the wrong sequence, the engines shut down and must be restarted, which results in a delay at the gate, he said.

Boeing engineers were aware of the problem during the plane's flight tests, said Davis, but decided to maintain the plane's sales schedule and troubleshoot later.

Boeing also discovered a problem with the plane's central maintenance computer during flight tests. The computer, which keeps track of equipment malfunctions in 75 separate systems when the plane is on the ground, was not "fully debugged" when Boeing began delivering its first 400's last year, Davis said.

The 400's performance record lagged so badly behind previous jetliner models that the company formed a special task force last month to whip the plane into shape. Davis, who heads the task force, said the unit has started improving the 400's "dispatch reliability rate," the measure of how frequently the planes are delayed more than 15 minutes at the boarding gate because of mechanical malfunctions.

Davis said none of the problems encountered in the 400 could cause the plane to be unsafe to operate. But Boeing has received complaints "across the board" from airlines that own the jetliner, Davis said.

Boeing said it expects to cure the glitches in the 400 by making changes on its production line next month. ... So far, about 20 of the (57) 400's already in operation have been retrofitted since October. After the modifications, Boeing said, delays of the 400's due to mechanical problems dropped to almost zero.

The 400's reliability rate is currently running at 94.5 percent. That compares with a reliability rate of about 97 percent for Boeing's 767, which Davis said has "roughly the same technical elements" as the larger 400. Boeing, said Davis, had expected the 747-400 to parallel the 767's reliability rate. ...

* Two 747-400 computers fail during landing approach; recall denied

Jon Jacky, University of Washington <ON@GAFFER.RAD.WASHINGTON.EDU> Mon, 25 Jun 1990 17:59:07 PDT

Here are excerpts from THE SEATTLE TIMES, June 23, 1990, p. A11:

BOEING DENIES RECALL OF JET SOFTWARE --- Associated Press

Seattle --- A Boeing Co. spokeswoman yesterday denied a report by a Japanese news service that the aircraft manufacturer was recalling some cockpit computer software for its new 747-400 jumbo jets. ...

Kyodo News Service reported that on April 3, a pair of flight management computers on a Japan Airlines 747-400 failed to function when the plane was preparing to land in Seoul. JAL officials would not confirm the reported Boeing recall, but said both flight management computers on the JAL plane briefly failed to function properly as the plane was approaching the South Korean airport. ...

Kyodo, quoting unidentified industry sources, said yesterday that there was a programming problem in software for the 747-400's flight management computer, which controls such functions as navigation and flight planning.

The sources said Boeing would replace the software with an improved version after receiving permission from the Federal Aviation Administration, Kyodo reported. ...

"There has been no recall of FMC software," said Liz Reese, Boeing Commericial Airplane Group spokeswoman. Boeing is, however, in the process of issuing an updated version of the software, something it does about every six months as part of a regular plan for all 747-400 operators, she said.

The scheduled upgrade is separate from another Boeing program to fix bugs that appeared in software for other 747-400 computer systems, Reese said. ... In addition to the FMC, other computers monitor such things as the aircraft's environment, engines and maintenance needs. ... (When) the new jumbo jet went into service last year, operators reported "really nagging, minor problems," with bugs in some computer software, Reese said. In some cases, the software was sending out "nuisance messages," or reporting problems that didn't exist, she said. Boeing formed the "747-400 Task Force" with the operators to correct the problems and has been sending out improved software to fix the bugs, she said.

The 747-400, the world's largest passenger aircraft, is distinctive ... for its use of highly sophisticated computer systems that permit a flight crew of two, with no flight engineer. ... Introduction of the 747-400's was delayed from 1988 to early 1989. Boeing said it fell behind (...for various reasons, including) the plane's new electronic cockpit took longer than expected...

Re: The A320's attacks of nerves

Robert L. Smith <rlsmith@mcnc.org> Tue, 26 Jun 90 22:19:59 EDT

I'm afraid Robert Dorsett is mistaken when he states "And nobody's crashed a 757/767 yet. . ." On July 23, 1983, a 767 operating as Air Canada Flight 143 crashed at Gimli, Manitoba. That crash may well have been a proper "risk" subject. It seems the plane ran out of fuel while at 41,000 feet because someone inputted the wrong fuel load quantity to one of the flight computers.

This crash was well dramatized in "Freefall", by William and Marilyn Hoffer, St. Martin's Press, New York, 1983.

rLs
Kiskier Risks of Reading Risks (Re: Dancy, <u>RISKS-10.11</u>)

Michael Barnett <mbarnett@cs.utexas.edu> Tue, 26 Jun 90 11:42:11 CDT

I understand Keith Dancey's complaint about the "labelling" of articles, and I appreciate that some of the articles are often outlandish enough to provoke disbelief in their veracity. But it seems as if one of the greatest risks facing us today is the loss of a sense of humor (as well as a sense of proportion). Without intending anything personal, I cannot conceive of anyone reading the original article without realizing it to be a joke. Save us from a world where everything is labelled in advance so we can decide in advance how to react!

Mike Barnett, The University of Texas at Austin

Ke: "Unbreakable Math Code Finally Broken"

Y. Radai <ADAI1@HBUNOS.BITNET> Wed, 27 Jun 90 15:54:14 +0300

In <u>RISKS 10.11</u> there appeared a Washington Post article beginning as follows:

>Two mathematicians, working with hundreds of colleagues, announced yesterday>that they had broken a code viewed by many cryptographers and security experts>as virtually impenetrable. The feat, in which the mathematicians factored one>of the world's ``most wanted'' numbers, means that many security-minded>organizations will need to change their cryptographic systems to prevent>security breaches.

I don't know if this is another case of deliberate distortion in order to make things sound sensational or a misunderstanding by a reporter who doesn't understand the subject. In any case, it's grossly inaccurate. According to experts in the field, what Lenstra and Manasse (the two mathematicians who organized the factoring project) actually did was to factor a 155-digit number HAVING A VERY SPECIAL PROPERTY, namely one that equals $a^b + c$ where a and c are small (in this case a=2, b=512, c=1). The method used (a specialized version of the Number Field Sieve algorithm) does NOT apply to other numbers (which would be necessary in order to break a cipher such as RSA), and if another method, the Quadratic Sieve algorithm, were used, it is estimated that it would require 6.7 x 10^19 operations to factor a number of such length, which would take over 20 years if you had a machine which could perform 100 billion operations per second.

So the statements that an impenetrable code has been broken and that organizations need to change their cryptographic systems because of this achievement seem a wee bit exaggerated.

> Y. Radai Hebrew Univ. of Jerusalem, Israel RADAI1@HBUNOS.BITNET

Kisks involved in the new DEC RA90 firmware upgrade procedure

Geoffrey Brunkhorst <gbb@woz.mayo.edu> Tue, 26 Jun 90 16:49:06 CDT

A reprize on the 'burning your bridges' method of software/hardware upgrades...

Recently, a DEC software distribution required that all RA90 drives connected to an HSC (Hierarchical Storage Controller) were required to be at least at MicroCode Version MV10. Mine was at MV7 so I requested an DEC Field Service Service Call to replace the microcode. I was surprised to see that the this was really just software load off a special Zero Insertion Force slot on the RA90's console board. Just plug it in, hit the down-load command and the firmware is loaded (btw, the module was very sexy in its special plastic mount ;-).

The FS person proceeded to do the download. It failed on the verify pass.

Repeating the procedure generated the same result. The DEC FS person asked nicely if he could try the other R0A90 drive to see it would work there. I just as nicely said no, thank you.

Since the procedure apparently erased the EEPROM containing the old microcode, the drive was essentially broke. DEC has neglected to provide a 'backup'. Old firmware revisions left you with the old chips, or a floppy (ala 11/780 WCS upgrades) that contained the original downloaded binary. This new procedure apparently was not thought to be 'risky'.

Since it was 5pm, and the disk was a scratch disk, we went home for the evening, or so I thought. My FS person actually drove 2 hours to get the local DEC disk expert out of bed and down to the office to shake out the problem. He got home at 1am (confirmed. I happen to live next door to my FS person... sometimes handy, but our wives don't care for it that much ;-).

DEC's drive people confirmed that the data path from the load module to the EEPROM does not have a non-destructive self-test, and probably in our case had a broken part somewhere along the path. The only quick fix was to send down a new board, with good firmware on it, and replace the other parts (console module, and data cable), and hope everything was fixed.

The next morning we tried two boards. One 'old model' (fits only the RA90) did not fit (??). The new RA90/92 board, worked fine. Since there were at least 2 other parts that could cause the firmware load to fail, and the only way to test it was to risk destroying the working firmware with possibly no recovery (DEC couldn't be sure on that), I vetoed any further testing, in lieu of a more formal shakedown at some later date. I got to the required rev, albeit over 17 hours after the upgrade started.

Given the amount of data on a RA90 (1.2 GB, 1.5+GB on a 92, which uses the same procedure/hardware), the amount of downtime it causes when a firmware load fails, it strikes me a a great risk to a) erase the eeprom first (given its nature, putting an equal amount of dram and downloading to that, and if successful, then loading to EEPROM would be a better solutions) and b) to not

have a 'backup' to roll out the eeprom data (again, a dram, or at least a write command, which would essentially test the data transfer path in a nondestructive manner).

Geoff Brunkhorst

info on carpal tunnel syndrome (CTS)

Jim Meyering <meyering@cs.utexas.edu> Wed, 27 Jun 90 09:40:34 CDT

[Submitted via werner@cs.utexas.edu (Werner Uhrig)]

A friend suggested I read the following message (once posted to the sci.med newsgroup).

I think it should interest anyone who types a lot.

One point the author does not mention is that the "force-depression curve" of your keyboard may also play a role. It is better to have a linear relationship between force and depression. But the keys on some keyboards require greater force to depress the first few millimeters than the last few. This gives what is sometimes hyped as "positive-touch" or something similar. The net result is that you have to press (relatively) hard to get over the "hump," then with the low resistance beyond it, your fingers bang into the base with more force than with "linear" keyboards. People have suggested that this sort of dynamic may aggravate or even induce CTS. Many of our HPs have this "nonlinear" keyboards. The keys on some Sun3 keyboards have become so sticky that they give the same effect.

Jim Meyering meyering@cs.utexas.edu uunet!cs.utexas.edu!meyering

From: Andrea Frankel <andrea@sdd.hp.com>

Carpal Tunnel Syndrome:

This is a slightly edited reposting; apologies if you've seen it before, but many people who read this on an internal HP notes group have found it useful and asked for it to be more widely distributed.

Disclaimer: I am not a doctor (but I sometimes play one on the Net ;@). This is from my own personal experience with the malady, supplemented by a little research and lots of talking to doctors and such. Carpal Tunnel Syndrome is being seen more and more frequently among the computer set (my neurologist jokingly refers to it as "hacker's hand"); when caught early, conservative treatment can completely cure it. However, if you let it go on long enough you can cause irreversible damage. If you have any question at all, PLEASE SEE A DOCTOR! Better safe than sorry.

1. The setup

The bones in your wrist form a 3-sided tunnel, with the fourth side closed off by a very tough piece of cartilage. In this carpal tunnel run the tendons of the muscles which flex your fingers, as well as the very important median nerve which ennervates the thumb and the first two fingers.

If something happens to cause the contents of the tunnel to swell, or to cause the tunnel itself to get smaller, the pressure exerted on the median nerve results in carpal tunnel syndrome. Pregnancy, sudden weight gain, drugs which cause water retention, and repetitive overuse (or abuse) which causes tendinitis in those flexor tendons, can all cause carpal tunnel syndrome. (I recently learned that hypothyroid condition can also cause CTS.)

Positions where the wrist is bent back while being used really exacerbate the problem (e.g. bicycling with drop handlebars, if you are not careful about hand positioning).

Other things can contribute as well - if you are doing carpentry in your spare time and twisting many screws by hand, for example. When you become aware of the problem, start becoming aware of both the wrist position and the stresses on it in various activities.

The median nerve runs up the heel of the hand onto the palm, along the "life line". Direct repeated blows to this area can mimic or add to the carpal tunnel syndrome, and are often lumped in with it. Our HP keyboards are awful in this respect. Kayaking, bicycling, gardening without heavy gloves, all sorts of things can bang on this exposed nerve.

2. The symptoms and diagnosis

Any or all of the following: pain, numbness, tingling, or sensations of fullness in the fingers, hands, or shooting up or down the arms.

Quick test #1: make an "O" with thumb and forefinger, insert the thumb and forefinger of the other hand, and resist while trying to force the "O" apart with the other hand. The "O" should not come apart!

Quick test #2 (Tinnel sign): place the backs of your hands together, bend each hand 90 degrees towards the inner wrist, fingers pointing down (forearms parallel to the floor, held out in front of you).

=====oo======= key: === forearms

 Image: one of the second secon

Press the backs of the hands together and hold for 30-60 seconds. If you start getting some numbness or tingling or pain, this is suspicious.

Loss of grip strength is a sign that you may have a more advanced case.

(I finally sought help when I was unable to open a can of tuna fish with a standard Swingline manual can opener.)

I believe the best specialist for diagnosis is a neurologist. A neurologist will do nerve conduction studies, comparing rates of conduction above and below the wrist, and between hands. A good one will also do electromyography, to see if the muscles enervated by the nerve are firing properly or not. (As a techie, I was fascinated to watch the 'scopes while he poked me!)

3. The treatment

Standard treatment is to start with the most conservative, least invasive approaches, and move up only if they don't help. The old RICE formula - rest, ice, compression, and elevation - is the place to start, but omit the compression as this is not a muscle strain.

A wrist splint (basically a velcro-and-ace-bandage type of thing with a bent metal strip in it to hold the wrist in the right position) is worn at night for a month to see if it helps; it can also be worn during the day for stretches. (Do not make it tight - it is for positioning only.) In many cases, that plus correcting one's work habits is sufficient. Some people find that a month is all it takes; others use the splint at night for the rest of their lives, or off and on as needed. I still use mine occasionally when I've been overdoing it. It's also a good idea to wear it in situations where you might be tempted to do something silly (like lugging suitcases or lifting weights), both as protection and as a reminder to be careful.

Non-steroidal anti-inflammatories (e.g. Motrin) are used, if it looks like inflammation is a major cause of the problem.

Icing the wrist helps alot, both for the pain and the swelling. (Be aware that over-icing has a rebound effect as the body attempts to warm the area by increasing circulation. Best is to ice for 10-20 minutes max each time, leaving at least an hour between icings.) I keep a couple of the soft gel-type blue ice packs in a little fridge near my desk, so that I can ice several times a day if I need to. Bags of frozen peas work great (hit 'em a couple whacks on the counter to loosen them up, then pat the bag around your wrist so it conforms to the curves). For obvious reasons, jacuzzis (especially if you leave your arms in) will tend to make things worse.

If water retention is a problem, you might try a mild OTC diuretic. (Women: it isn't uncommon for CTS symptoms to be worse during PMS time.) Also, simply elevating the wrist (for example, resting it on the back of a padded chair or car seat, or sleeping with your splinted wrist wresting next to your head on the pillow) can help relieve some of the discomfort at least temporarily by reducing the swelling.

As a long-time fan of vitamins, minerals, and Prevention magazine, I of course asked my doctors about B6 as a treatment for CTS. Unfortunately, the original article reporting success from B6 treatment was not reproducible by other experiments. What's more, excessive doses of B6 (over 50 mg/day supplement to a normal diet) can actually cause peripheral neuropathy, mimicking some of the symptoms of CTS. My doctor said it wouldn't hurt if I wanted to take up to 50 mg/day, but since I had been taking that amount for quite some time for other reasons, he advised against increasing it.

Some doctors go for cortisone injections, although mine cautioned that the carrier substance is not well absorbed, and can actually make the problem worse by increasing the fluid pressure in the tunnel. Your doctor will decide based on the type of CTS and how it is responding to other treatment (or not).

The final stage is surgery. I had mine a few years ago; if you're facing it, I'd be glad to chat with you about it. The surgery itself was a piece of cake, taking maybe 10 minutes once I was fully prepped - very simply, they slit that piece of cartilage along the "life line" and onto the wrist, and it spreads apart before it heals up, making the tunnel larger. Instant relief, although the recovery and rehab takes a couple months. For those interested in such things, I talked them into skipping general anaesthesia in favor of a Bier Block, which worked splendidly - I was out of there and wolfing down antipasto and garlic bread an hour after surgery.

A friend notes that not everybody who has had the surgery finds it a piece of cake. His advice would be to make sure you have absolutely the best doctors when it come to surgery on one's hands, with which I heartily concur! Hands are incredibly complex, considering all the different types of finely coordinated movement they are capable of (and all the muscles and nerves that requires).

I would strongly recommend that you look for an orthopedic surgeon who is board certified in Hand Reconstruction Surgery - my scar is almost invisible, compared to some pretty horrific looking ones I've seen. (I asked the neurologist, who was really top-notch, to look through my CCN [preferred provider] booklet and recommend someone to me.) An orthopedic surgeon who handles a little bit of everything - shoulder tears, knee arthroscopy, back problems - probably won't be as good at carpal tunnel surgery as someone who spends their entire professional life specializing in the elbow down. For example, my surgeon stopped the surface cut at the first wrist fold, lifted the skin, and continued the surgery under the skin to minimize the scarring; other surgeons (who don't specialize in hand reconstruction surgery) often don't think to do that. It doesn't affect how effective the surgery is, but it sure makes a difference in how pretty your hand looks afterwards!

4. The progression

The symptoms may come and go with heavy bouts of typing, bicycling, etc. When it gets really bad, it can hurt all the time or start aching spontaneously.

In the early stages, relieving the pressure on the median nerve will quickly reverse the symptoms (in a matter of days to weeks).

Untreated, the pressure on the nerve will eventually cause it to die back to the point of constriction. When this happens, the muscles atrophy. (The large adductor which forms the mound at the base of my thumb had shrunk to half its size by the time I was operated on.)

If you don't catch it quickly at that point, the nerve sheaths (which the nerve had been inside before it died back) start to fray. This is bad news. If you have surgery while the sheaths are still intact, the nerve will grow back along the sheath (around 2 mm/day - you can actually track it!) and pretty much recover all of its connections and functions. I have a tiny patch less than 1/4" diameter on two finger tips which is numb, and otherwise have full function back. If the nerve sheaths have frayed, however, the nerve can't find its way back to make the right connections, and you're screwed.

IF YOU THINK YOU MIGHT HAVE CARPAL TUNNEL SYNDROME, GET IT LOOKED AT *NOW*!!! Don't delay, or you might not make a full recovery. Workman's comp studies looking at prognosis for recovery give very low odds, based on most factory workers (who used to account for most of the CTS claims before computeritis hit) being too macho or too scared of losing their jobs to file a claim before it was too late.

5. Prevention

The optimal position for your wrist is with the hand bent back just 20-30 degrees; you want the position where the front of your wrist makes a straight line with the first inch of the heel of the palm. Play with it a bit until you find the place where the wrist seems to be maximally "open", but without bending the hand back so far that you feel strain.

Look down at your hands as you type - if you are dropping your wrists, you are at risk. Think about how they used to teach piano technique: an almost straight line along the back of the forearms, through the wrist, onto the back of the hand; fingers dropping down. (My sister's piano teacher used to place pennies on the back of her hands while she played, to teach keeping it level.) Practice typing that way, and instead of resting the heel of your hands on the edge of the keyboard when you're thinking or reading, rest them in your lap instead.

I got a very nice padded wrist rest from a local office supply house, that allows me to rest my forearms or wrists while I type in this position; I have one under my 320 keyboard, and one for my Vectra. You can also improvise by taking a length of bubblewrap, rolling it up and securing the ends with rubber bands, then taping the roll to your desk in front of the keyboard. Warning: this padded wrist rest can actually make it worse for some people, if it distorts the normal typing motion or presses too hard against the wrist.

I currently have a keyboard draw from Devoke (about \$115) that has a full 6" height adjustment, slides in and out and swings to both sides. It mounts with two screws, and I have one in the "L" of my workstation

table at work, and on the desk at home where I have my PC. This has made the most difference when my CTS flared up again (along with rest and splinting).

Wear padded gloves for anything which might bang on your hands. Bicycling gloves with Spenco pads can be used for many things (I wear mine ice skating!). The Spenco pads are definitely superior to leather or other types when it comes to cushioning that area against shocks. (After the surgery, I was warned that the median nerve would always be a bit more exposed and sensitive, and it definitely made me a connoisseur of bicycling gloves!)

Learn to back off when you realize you're about to lift or torque something heavy with your wrist bent. If you can't rethink the movement so you can keep your wrist straight, get help (person or tool)!

p.s. Feel free to copy and distribute this to anyone who might be helped. I only request that you not delete anything, especially the disclaimer.

Andrea Frankel, Hewlett-Packard (San Diego Division) (619) 592-4664 UUCP : {hplabs|nosc|hpfcla|ucsd}!hp-sdd!andrea USnail : 16399 W. Bernardo Drive, San Diego CA 92127-1899 USA



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Theodore Lee <lee@TIS.COM> Wed, 27 Jun 90 22:19:44 -0400

MESSAGE FROM RON RIVEST VIA JIM BIDZOS VIA STEVE KENT VIA STEVE CROCKER: Thanks to Robert Silverman for keeping many people honest. As an additional effort to that end, I attach an analysis of the recent factoring effort, done by Ron Rivest. The early reports of RSA's demise have been greatly exaggerated... Note: Be sure and read the end of Rivest's note. Jim Bidzos, RSA Data Security To: Whom It May Interest (Feel free to distribute further...)
From: Ronald L. Rivest
Date: June 21, 1990
Re: Recent Factoring Achievement

(Preliminary draft; may contain typos or other inaccuracies.

Please send corrections to rivest@theory.lcs.mit.edu)

This note is in response to the numerous inquiries I've received regarding the recent factoring of a 155-digit number by A. Lenstra, M. Manasse, and others. (See the New York Times article of 6/20/1990 by G. Kolata.) This note attempts specifically to correct some of the misimpressions that may arise from a reading of such popular press articles.

Using an ingenious new algorithm, Lenstra, Manasse, and others have factored the 155-digit number known as "F9", the ninth Fermat number:

 $F9 = 2^{(2^9)} + 1 = 2^{(512)} + 1$.

In binary, this number has the form

100000....000000001

where there are 511 zeros altogether. (F9 is a 513-bit number.) This is a fascinating development, and the researchers involved are to be congratulated for this accomplishment.

The algorithm used is known as the "number field sieve", or "NFS" (not to be confused with a network protocol of the same acronym!). The NFS algorithm is described in the Proceedings of the 1990 ACM STOC Conference. The NFS algorithm is based on an idea due to Pollard, as developed further by Arjen Lenstra, Hendrik W. Lenstra, and Mark S. Manasse.

The NFS algorithm is specifically designed to factor numbers that, like F9, have a very simple structure: they are of the form

a^b + c

where c is relatively small. (For F9, we have a=2, b=512, and c=1.) Some simple extensions of this algorithm are also possible, to handle numbers whose binary representation has many zeros, and related kinds of numbers (ternary, etc.) Numbers that have such a special structure are extremely rare and are unlikely to be encountered by chance. That is, the NFS algorithm does not apply to the kind of "ordinary" numbers that arise in practical cryptography, such as using RSA. They only apply to numbers with "sparse" representations having few nonzero components. (Let us call such numbers "rarefied".)

When working on a rarefied number, the NFS algorithm has an estimated running time of the form (for an input number n):

exp(1.56 (ln n)^1/3 (ln ln n)^2/3) (1)

For n = F9, this evaluates to

4.1 x 10^15 operations,

which, at 3.15 x 10^13 operations/year for a 1 MIP/sec machine (i.e. a MIP-year), gives a workload estimate of

130 MIP-years,

only off by a factor of two from the actual work of 275 MIP-years. (That is, formula (1) may be roughly too low by a factor of two.)

It is instructive to see the effect of doubling the size of the number being dealt with. A 1024-bit (332-digit) rarefied number requires an estimated

1.54 x 10²¹ operations

= 4.9 x 10^7 MIP-years,

a dramatic increase in difficulty. The NFS algorithm algorithm is not a "polynomial-time" algorithm; the difficulty of factoring still grows **exponentially** with a polynomial function of the length of the input.

What has this to do with RSA and cryptography? I think there are three basic points:

- -- This development indicates that the status of factoring is still subject to further developments, and it is wise to be conservative in one's choice of key-length.
- -- The NFS algorithm may yet be generalized to handle "ordinary" numbers, and the potential impact of this should be considered.
- -- Factoring is still a very hard problem, despite everyone's best efforts to master it.

Regarding the further extensions of NFS to handle ordinary numbers, this is judged to be a reasonable possibility by those working on NFS, so it is helpful to consider what impact this may have.

It is conjectured (see the ACM STOC paper referenced above) that a successful extension of the NFS algorithm to ordinary numbers would have a running time of the form:

 $exp(2.08 (ln n)^{1/3} (ln ln n)^{2/3})$ (2) This is similar to equation (1) except that the constant 1.56 is replaced by the constant 2.08. Note that a practical version of such an extension does NOT yet currently exist (to the best of my knowledge), but even granting its plausibility we arrive at an estimate of the tie required to factor a 512-bit number of

6.5 x 10²⁰ operations

= 2 x 10^7 MIP-years

which (in my opinion) is a substantial degree of security. It is interesting to note that this work factor is actually GREATER than that required by the ``standard'' factoring algorithms (e.g., the quadratic sieve), which have a running time of

exp((ln n)^1/2 (ln ln n)^1/2);

for a 512-bit number, this gives a work-factor estimate of only

6.7 x 10¹⁹ operations.

Indeed, the NFS algorithm (when extended) will be asymptotically superior than the quadratic sieve algorithm, but will be slower for numbers with less than about 200 digits. That is, assuming that (2) is indeed the correct running-time estimate for any extension of NFS, then NFS will not affect the security of any numbers of less than about 215 digits. So any "standards" that have been considered using 512-bit RSA moduli are not likely to be affected by any NFS extensions. (At most, one could imagine that the RSA key-generation process might be extended to check that the resulting modulus n is not a rarefied number.)

In the truly worst-case scenario, we would have that an extension of NFS would be found that allows ordinary numbers to be factored with a work-factor that is governed by equation (1); in this case one would need to adjust the sizes of moduli used by RSA upwards by a factor of less than two to more than offset the new algorithm. A factor of two

in size affects the running time of public-key encryption (or signature verification) by a factor of four and the running time of private-key encryption (or signature generation) by a factor of eight. Noting that the speed of workstations has increased by a factor of over 100 in the last decade (indeed, such factors have been the technological advance that made the successful implementation of NFS possible!), such performance penalties, if necessary, seem to be easily absorbed by expected technological advances in the speeds of the underlying RSA implementation technologies. That is, the NFS-like factoring algorithms do not, even in this worst-case scenario, prevent successful implementations of the RSA cryptosystem.

As a cryptographer, I am actually very happy with all the effort that is being spent trying to determine the exact level of difficulty of factoring. Achievements such as the recent development of NFS help to pin down the best-possible rate of growth of the difficulty of factoring, so that users of cryptographic schemes can pick key sizes with an increased degree of confidence that unforeseen developments are unlikely to occur. The best way to ensure confidence in a cryptographic system is to have it attacked vigorously and continuously (but unsuccessfully) by well-qualified attackers. If, despite their best efforts, the difficulty of cracking the system remains intrinsically exponential, then one can have a reasonably high degree of confidence that the system is actually secure. This is the process we have been seeing at work in the recent work on factoring. The results of the attacks can be used to guide the selection of the necessary key size for a desired level of security (with an appropriate margin of safety built in, of course).

(As a closing note, here's a prediction: I expect that the 128-digit ``challenge RSA cipher'' published in the August 1977 issue of Scientific American to be cracked (probably by the quadratic sieve algorithm or a variant, not NFS) during the next 1-3 years. This accomplishment will require substantially more computer time than the 275 MIP-years required to factor F9.)

Kisks from using laptops with cellular phones

Jan I Wolitzky <wolit@mhuxd.att.com> Thu, 28 Jun 90 10:01:35 EDT

I'm concerned by the increased use of laptop computers with cellular phones, to connect to remote host machines. Given the ready availability of scanner radios capable of receiving cellular phone frequencies, this practice seems to amount to broadcasting your passwords, proprietary information, etc., to anyone who cares to listen. (Yes, I know that federal law prohibits listening to such calls, but everyone who has a scanner or knows someone with one knows that it's done all the time.) Is there any record of anyone breaking systems this way yet? Has any company adopted a policy discouraging its employees from using laptops with cellular phones, or, for that matter, from broadcasting other sensitive information over cellular phones?

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 201 582-2998 att!mhuxd!wolit or jan.wolitzky@att.com (Affiliation given for identification purposes only)

Ke: info on carpal tunnel syndrome (CTS) (<u>RISKS-10.12</u>)

Mike Tanner <tanner@cis.ohio-state.edu> Thu, 28 Jun 90 09:06:49 -0400

At the risk of turning this into a medical forum I wanted to add to the excellent summary on carpal tunnel syndrome that there is a related problem called ulnar nerve syndrome. As with CTS, those of us who spend lots of time using keyboards are prone to ulnar nerve syndrome, too. The main difference in the symptoms is that with CTS the numbness and tingling is in the thumb and first two fingers, with UNS it is in the other two fingers and along the outside of the forarm. (When you "hit your funny bone", what you've done is bash your ulnar nerve. The symptoms are similar to that feeling, but they don't go away.)

My wife's neurologist (she's been going through a bout of it) said there are many causes, but a common one is some activity that constantly rubs the elbow. In her case it is almost certainly typing while resting her elbows on the arms of a chair. One danger is that carpal tunnel syndrome is so hot, such a fad right now, that a physician might automatically connect "numbness" with "programmer" and say "carpal tunnel". My wife's physician did this, and only changed his mind after we had looked in some medical books and found that CTS symptoms did not match hers. (Physicians deny that they reason this way. Experience tells otherwise.)

Treatment is basically like CTS: ice, avoid bending the elbow as much as possible (not easy to do), don't do things that rub the elbow a lot, anti-inflammation drugs. There is surgery, but unlike CTS, ulnar nerve surgery is not a good option. Apparently it has about a 50% chance of making things worse, according to my wife's neurologist. (That might have been an estimate that took the nature of her condition into account, i.e., there are cases where it has a high probability of success, but hers isn't one of them.)

-- mike

Ke: info on carpal tunnel syndrome (CTS)

<henry@zoo.toronto.edu> Thu, 28 Jun 90 14:11:52 EDT

>One point the author does not mention is that the "force-depression curve" of
 >your keyboard may also play a role. It is better to have a linear
 >relationship between force and depression...
 >... People have suggested that this sort of dynamic may

http://catless.ncl.ac.uk/Risks/10.13.html[2011-06-11 08:06:57]

>aggravate or even induce CTS...

What was the incidence of CTS twenty years ago, when electric typewriters routinely had non-linear force-depression curves? Or before that, when manual typewriters required far more finger pressure than any modern keyboard? Yet again, we have here a case of a "computer risk" that isn't really new, and data from olden days could be very useful in deciding what *really* causes it.

Data would be particularly useful because it's easy to construct an argument that points in precisely the opposite direction! Once you've pushed a non-linear keyboard key "over the hump", you can relax pressure. But with a linear keyboard, you have to push all the way down, since you get no "that's enough" feedback until the key hits bottom.

Some of this may be a risk not of nonlinear keyboards, but of lack of proper training. Pre-computer typing courses taught you to *strike* the keys rather than *pushing* them, so your muscles were already relaxing when the key bottomed out. One side effect of the proliferation of keyboards is that far more people are using them without formal training, or with training from "touch typing" programs that teach you which keys to hit but don't teach posture or hand position.

Henry Spencer at U of Toronto Zoology

Ke: The Hubble Telescope (<u>RISKS-10.10</u>)

<henry@zoo.toronto.edu> Thu, 28 Jun 90 00:01:37 EDT

> Tonight's news was really distressing -- that there is a fundamental> mirror flaw that cannot be repaired until 1993 or so.

It's not *quite* that bad. The optics do seem to have a significant case of spherical aberration -- so perfect that it's almost certainly the result of an incorrectly-figured shape, rather than a manufacturing deviation from the desired shape -- and this will hurt the cameras badly, but the spectrographs and the photometer (3 out of 5 of the instruments) shouldn't be badly affected. Unfortunately, the affected instruments are the ones that would produce all the nice crowd-pleasing pictures, so the public-relations disaster is much worse than the scientific one.

The Wide Field / Planetary Camera was slated for replacement in 1993-4 anyway, and it may be possible to build the replacement in time for a 1991 flight (about the earliest NASA could launch a repair mission anyway).

The big question is, how did this happen?

Henry Spencer at U of Toronto Zoology

utzoo!henry

×

Hubble telescope

<smb@ulysses.att.com> Thu, 28 Jun 90 16:49:21 EDT

The Hubble space telescope, which cost \$1.5e9 to build (and a lot more to store and launch), isn't working properly. There appears to be a problem with one of the two mirrors being flawed. Weren't they tested? Yes, they were -- but they were tested individually, not in the final assembly. It seems that the test jig would have cost too much.

Lessee -- the components all worked individually, but not as a system. Where have I heard that one before?

--Steve Bellovin

My A320 "Article"

Gregory TRAVIS <greg@cica.indiana.edu> Mon, 25 Jun 90 21:51:33 EST

Just to get the record straight, I originally wrote and posted the entire story to rec.aviation, a newsgroup I felt would appreciate the humor without undermining the serious aviation-related discussions also posted there.

I considered submitting the story to RISKS orginally, but decided against it because of the harm it might have done to RISKS serious nature. Robert Dorsett, I believe, passed the submission on to RISKS (through PGN?) much to my delight. Personally, considering the flood of mail I've received, I think we might well start a serious discussion in RISKS about the risks of computer types who cannot recognize a blunt-faced satire when it hits them.

Gregory Travis

Ke: The A320's attacks of nerves

Robert Dorsett <rdd@ccwf.cc.utexas.edu> Wed, 27 Jun 90 21:50:44 -0500

Robert L. Smith <rlsmith@mcnc.org> wrote:

I'm afraid Robert Dorsett is mistaken when he states "And nobody's
 crashed a 757/767 yet. . ." On July 23, 1983, a 767 operating as Air
 Canada Flight 143 crashed at Gimli, Manitoba.

Actually, it's difficult to classify that as a crash. Part of the difficulty is terminology: "crash" is not defined by either ICAO or the FAA. The two relevant terms are "accidents" and "incidents."

US NTSB 830-3 defines "aircraft accident" as "an occurrence associated with the operation of an aircraft which takes place between the time any person

boards the aircraft with the intention of flight and all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage."

"Incidents" are anything other than crashes, which could affect the future safety of operations.

The Air Canada landing at Gimli can certainly qualify as an accident. However "crash," as used by the industry in general, has more permanent connotations. The airplane was under control at impact, did not suffer substantial damage, and nobody was seriously injured. I therefore hesitate to classify it a crash.

On the other hand, there *was* a rather nasty incident in Florida a few years ago, a result of a "hard landing." The airplane was damaged sufficiently enough that it was a marginal-recovery issue, but it remained under pilot control, and nobody was seriously injured. Both the Gimli 767 and that 767 are back in the air.

Perhaps I should rephrase my original comment: there have been two A320 hull losses. There have been no 757 or 767 hull losses.

> That crash may well have been a proper "risk" subject.

Indeed; it's been popular in the past. Here's the review of _Freefall_ I posted to rec.aviation last year. It may be of interest to RISKS readers.

=====

Freefall (by William and Marilyn Hoffer, St. Martin's Press: New York, 1989) deals with the near-crash of Air Canada Flight 143, a Boeing 767-200 which ran out of fuel over near Winnipeg, Manitoba in 1983.

The book is partially investigative reporting, partially schlock: while it provides a detailed accounting of the events leading up to the eventual landing, it also wastes an enormous amount of space on what the passengers think, feel, etc--and in that respect rather closely resembles the style Arthur Haily used in _Airport_. In other words, it's light reading, and tries to be something for everyone. Fortunately, though, the authors kindly segregate the chapters into what's happening in the cockpit, and what's happening elsewhere. If one sticks to the "Cockpit" (clearly labelled) chapters, it's tolerable (but since the book itself is only 263 pages of double-spaced large print and large margins, and less than half of it deals with the technical issues, the \$17.95 price tag isn't exactly worth it).

To save people the some time and effort, here's what it boils down to:

1. A fuel-metering device failed on a previous flight. A maintenance worker, through trial and error, got the system to work again. A subsequent worker mistakenly flagged the system as inoperative.

2. To verify how much fuel was on board, "dripsticks," a series of fuelmeasurement devices mounted under the wings, were used. A flotation device ("donut") is mounted on the top of the stick; when the stick is released, it drops. Where it stops (a length unit, represented by how much of the stick is pointing out) can be used to determine how much fuel is in that compartment. The procedure then is to use a chart to convert the unit read into liters, then to kilos, then, finally, to use a conversion factor to get pounds. All such measurements are then added to determine the total load on board. In Flight 143's case, an incorrect conversion factor was used for the last step. Confusion among ground workers and the flight crew as to the correct conversion factor (the 767 was the only metric aircraft in Air Canada service) induced them to launch with half tanks.

3. The captain launched with his fuel metering system inoperative, in violation of the minimum equipment list (but there may have been justification for doing so, as several references contradicted each other on this point). To overcome the loss of the totalizer, they set the flight management system with what they thought was a full load, which then provided them with a fuel burn total for the rest of the flight. GIGO.

4. They ran out of fuel near Winnipeg, Manitoba, which resulted in a loss of nearly all of their electrical power, including the EFIS and EICAS systems (electronic flight instrumentation and engine control and monitoring instrumentation). Radios and backup instrumentation was supplied by battery power (and, initially, APU power); some hydraulic power was obtained from a ram air turbine (optional equipment, I believe, on the 767--Air Canada bought them in anticipation of extended-range twin oceanic operations). The turbine serviced basic flight controls, but did not provide power for other surfaces, such as flaps. They were eventually forced to deadstick the plane to an abandoned military base near Gimli. They landed on top of a social event being held on a disused runway, fortunately not killing anyone. The nose gear collapsed, there was a small fire (from the nose brakes) and there was some damage to the airplane, but the plane was eventually put back in service.

5. The flight crew was initially fired, then rehired. The first officer, according to the book, is starting his captain's training.

🗡 The Gimli Glider

John (J.G.) Mainwaring <RM312A@BNR.CA> Thu, 28 Jun 90 09:52:00 EDT

Robert L. Smith in his posting re: the A320's attack of nerves refers to the crash of an Air Canada Boeing 767 at Gimli Manitoba. He seems to be using the word 'crash' in a sense with which I was previously unfamiliar.

The plane ran out of fuel because of a combination of factors. The fuel guages (computerized?) were malfunctioning, and Air Canada was in the early stages of conversion to metric. Reports at the time suggested that the refuelling was measured in pounds and the measurement was used un- or incorrectly converted in a formula that expected kilos.

When the engines flamed out, the rather small WW 2 training field at Gimli was

the closest airport, 100 miles away. The pilot was highly praised for making a successful dead stick landing, and the plane became known as the Gimli glider. I believe it was flown out a few days later, without the passengers and with a very carefully calculated fuel load.

The subsequent investigation was somewhat acrimonious, with the airline pointing out that the pilot had ultimate responsibility for the fuel on board, opposed by a strong public sympathy for the pilot and a feeling that the system was designed to fail. I suppose the risks are pretty much the same whether a computer was involved or not - large organizations occasionally screw up when they try to run complicated systems. This case also shows the value of properly trained people retaining ultimate control of the system.

Virus experiences in GDR

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 22 Jun 90 15:38 GMT+0100

On June 19-21, 1990, IBM held some kind of a development conference for GDR universities, in the research center of the ministry for science and technology in (east) Berlin-Koepenick. Similar to an annual conference for West German universities (`IBM university forum'), invited speakers from West and East German universities as well as from IBM informed about their actual work. A broad diversity of areas was covered, from CD-ROM based 'Thesaurus Linguae Graecae' to CAD, simulation of complex molecules and synthetic speech. The conference was accompanied by an exhibition where many additional applications and software products of scientific interest were shown by East and West German scientiests as well as IBM people, on IBM owned PS-2s. Many demonstration diskettes were freely available.

Among the exhibitors, the Virus Test Center demonstrated how to detect and eradicate viruses. In many discussions, we were surprised to learn that many scientists regarded viruses as some kind of a joke as they had suffered mainly from viruses of the funny kind, e.g. playing Yankee Doodle in the Bulgarian version "TP 44" or "legalizing marijuana"; only a few seemed to have experiences in really damaging viruses such as Israeli or Dark Avenger. Yet at the end of the exposition, our essential task was to eradicate some damaging viruses such as Dark Avenger (the Bulgarian "Eddie" which broadly migrates through Eastern Europe) from most of IBM's PS-2 as neither protection nor careful work had been practized nor prescribed.

With surprise we learned that there existed a secret research unit in GDR to which every virus or other threat had to be reported; this secret group would then produce an antivirus and send it to concerned institutions. In its latest version (which we hope to receive afterwards), 11 viruses could be detected and eradicated.

Lesson learned: there should be a special antivirus service for exhibitions, not only for large ones (in FRG's CeBIT and Systems exhibitions, about 15-20% of the workstations and PCs were found to be infected *at exhibition's end*).

Klaus Brunnstein University of Hamburg

A misdirected letter or Chain mail

GREENY <ISS026@ECNCDC.BITNET> Tue, 19 Jun 90 03:28 CST

Recently, the LISTSERV which I get my risks digests from sent me a copy of one of those unsolicited mailings that I always get via the US MAIL. You know the type, "You can make 50,000 bucks overnight with my ...". Yeah, yeah right. Those are one of the reasons (besides bills) why I dont go to my mail box any more, and deal with electronic mail.

Now I get to deal with this kind of crapola via the BITNET? Regardless of whether or not the message was accidently sent to a LISTSERV and redistributed to everyone that the LISTSERV knows about, I never should have been able to receive the message. LISTSERV software should be modified to include some sort of authentication. Granted, an individual with enough know-how can bypass a simple "authentic address" in the "Received From/By:" headers, but it would prevent those "whoops, I accidently did its...".

Maybe the author did, maybe he didn't. Either way, I really dont enjoy reading that stuff, and am sure that others don't as well. Also, the proposed scheme is a pyramid, and is quite illegal here in II. Anyone for prosecution?

Greeny

[Abuses of the BITNET and USENET RISKS addresses have happened before, although they could easily be blocked were it not for the intentional sandbox orientation. Fortunately for the rest of us, we did not see the abuse. The author did apologize to me that it was not intentional, however... PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



RISKS Forum <risks@csl.sri.com> Fri, 29 Jun 1990 13:34:45 PDT

for the next three weeks. There might be an issue or two, but don't bet on it. Keep sending in the good stuff in any case. Thanks. The Management

🗡 Hubble

Mark Bartelt <sysmark@orca.cita.utoronto.ca> Fri, 29 Jun 90 13:20:14 EDT

[This is a message from Dimitri Mihalas (dmihalas@altair.astro.uiuc.edu). Mark Bartelt, Canadian Institute of Theoretical Astrophysics]

in case you have not heard: from a reliable inside source i found out that the problem with ST is that the SOFTWARE driving the polisher was defective. the corrections for spherical aberration were put in with the wrong sign. consequently the mirror is not corrected for sph. abb., but has an added dose of it.

the error was not detected during testing because no test with collimated light was ever done. (editorial remark: unthinkable!) apparently this was a \$30M economy measure in the face of the Challenger accident. likewise none of the optics were ever tested in vacuum. the primary was and is "perfect" relative to the specified curve; but alas the specification was wrong. sigh.

from my amateur astronomer days (does that include 1990?) i recall that spherical aberration is EASY to detect with the foucault test, which is done with a pinhole, not collimated light. it is hard to believe that ANYONE could have made such a blunder..

the only reason that people know this much is that the same software was used for AXAF. the errors there were so huge as to be immediately noticeable, and when the software was corrected, the mirror was "perfect". i don't know whether the information from axaf was available prior to the launch of ST, but it seems that it had to be. in which case one wonders why PE didn't issue a "hold everything!".

the future: no chance of bringing the whole telescope down for a refit. best plan is to design compensating optics into the lightpath for future instruments: relatively easy to do. but that will still take 3-5 years.

i suppose it's "win a few, lose a few..." but i personally think that nasa, the government, and the people should stick it into PE and TURN it hard until they agree to refund the cost of the mistake and of the repairs. i'm sick of seeing defense and defense-related contractors get away with bloody murder and just get fatter and fatter on the profits.

back to theory dimitri

Ke: "Unbreakable Math Code Finally Broken"

Richard A. Schumacher <schumach@convex.UUCP> 28 Jun 90 18:02:18 GMT

Y. Radai <ADAI1@HBUNOS.BITNET> writes:

> So the statements that an impenetrable code has been broken and that >organizations need to change their cryptographic systems because of this >achievement seem a wee bit exaggerated.

On the other hand, the NPR report mentioned that the Bank of England was planning to use a 150 digit number as a key in a new transaction processing system, but changed it to something "much larger" when they learned of the 9th Fermat prime factoring.

More on the Risks of searching the Lexis fulltext database

<junger@cwru.cwru.edu> 29 Jun 90 16:25:00 EST

A while back I sent to RISKS an (itself rather buggy) description of a bug that turned up in the Lexis/Nexis database when I was doing date delimited searches in the library containing the fulltext opinions of the United States Supreme Court. A representative of Mead Data Central--the owner of the Nexis/Lexis service--has since contacted me to explain the nature of the bug and to assure me that it will be corrected on June 30.

In the first place, it appears that the bug is _not_ in the basic software that searches through the database for cases decided on, after, or before a specified date. Secondly, it is clear that the bug did _not_ cause me to miss any cases that I should have located, it just turned up some additonal cases that were not decided within the period that I was searching. That is the good news.

The bad news is that the problem relates to the way that the Lexis/Nexis system parses dates in the database and that the proposed fix will work only until the year 2000, at which time a new variant of the bug should cause real havoc.

Here is a corrected version of the type of search that exposed the bug:

Entitlement and date(aft 12/31/39 and bef 1/1/50)

That search, when conducted in the Supreme Court file, should find all opinions, and only those opinions, decided by the United States Supreme Court during the decade of the 1940's that contained the word `entitlement'. (Lexis warned me that it assumed that I meant after 12/31/1939 and before 1/1/1950.) As it happens, there are no cases that meet those criteria. But Lexis reported that it had found a dozen or so cases--cases that did contain the word `entitlement' but that were decided in the 1960's, 70's, and 80's.

It seems that a couple of months ago Mead Data Central decided to include the argued-date as well as the decided-date within the date field, and it is this enhancement that caused the bug. The fix that will be implimented this Saturday is to once again exclude the argued-date from the date field.

Since cases are not always decided in the same year that they are argued, including the argued-date in the date field will, of course, cause some cases to be reported as occurring in two different decades, which would be a nuisance. But that is only a miniscule part of the bug. The real problem occurs because some cases are argued on more than one date, so that the argued-date field would appear in the database as, say: "argued June 22-23, 1980" and the decided date field as: "July 3, 1980)." At first glance that would not seem to cause any problem. And it wouldn't, except for the fact that the Lexis system parses the date fields in the same way that it parses user input, and thus concludes that "June 22-23" means "June 22-1923". Thus our hypothetical case would have a date of July 3, 1980 (which is after December 31, 1939) and would also have a date of June 22, 1923 (which is before January 1, 1950). If that case--decided, you will recall, in 1980--contains the word `entitlement' it will turn up in my search for cases in the decade of the 1940's, and in my searches in the 1950's, and in the 1960's, etc.

I can understand why the system parses user input so as to interpret 1/1/50 as 1/1/1950--but I never dreamed that a system would parse its own data. According to the people at Mead Data Central, however, their system parses the data fields in exactly the same way that it parses user input. It seems that the Lexis/Nexis database contains texts--especially news reports--with dates in the form "nn/nn/nn". Today those dates are parsed as "nn/nn/19nn", but what is going to happen in the year 2000?

It would seem that ambiguous data in the data base will be much harder to find and fix than a software bug.

Peter D. Junger, CWRU Law School

Ke: info on carpal tunnel syndrome (CTS)

Terry Kane <tok@stiatl.UUCP> 29 Jun 90 19:36:47 GMT

I am a long time sufferer of CTS. The first symptoms I recall were during high school, nearly twenty years ago, but it was not properly diagnosed until I was in excruciating pain, dropping things, not sleeping because my hand was burning at night and more, all about four years ago.

Tests said that I had "a very mild case"!? That reassuring info did not make my hand better. I used splints, Motrin, ice until I finally insisted on the carpal tunnel relief operation. That was two years ago, this month, but I still have recurrences - especially when I meet the same RISK which pushed my CTS over the edge: using a MOUSE.

The typical mouse promotes all the bad habits that can result in CTS symptoms. One typically rests the heel of the palm on the mouse, and press the chord keys - frequently with constant pressure (on Apple's mice, the required pressure is substantial for me, and their new mouse reqlly aggravates the problem with its stylized, aerodynamic "look"). I cannot use a mouse to this day without suffering a "mouse hangover".

Track balls are better for me, but I still would rather avoid them.

I am really looking forward to _getting_my_hands_on_ ;-) a touch screen. I've seen some very nice ones with quite satisfactory resolution!

And please - If you think that you might have CTS - don't waste time. See Your M.D.

Terry Kane, Sales Technologies, Inc, Atlanta, GA (404) 841-4000





Brian Randell &rian.Randell@newcastle.ac.uk> Thu, 5 Jul 90 18:18:16 BST Readers of RISKs might be interested in a recent Oxford University Press paperback book "Benefits and Risks of Knowledge-Based Systems" (ISBN 0-19-584743-9). This is a 76-page Report of a Working Party of the (UK-based) Council for Science and Society, chaired by Professor Margaret Boden (Prof of Philosophy and Psychology at the School of Cognitive and Computing Sciences, University of Sussex).

The main chapter headings are:

1 How Knowledge-Based Systems Work

2 Applications of KBSs

3 The Benefits and Dangers of KBSs

4 Influencing the Future Uses of KBSs

5 Conclusions and Recommendations

Summarizing the final conclusions and recommendations:

1 The general level of public awareness about the applications and social implications of KBS is low, and education about KBS should be included in school courses.

2. There should be more interdisciplinary undergraduate and postgraduate study programs in cognitive sciences and KBSs.

3. A government initiative applying KBSs to health education and health care would be popular and in the long term cost-effective.

4. A KBS should complement human workers rather than replace them.

5. It is undesirable to substitute a computer for a human function, such as the giving of psychiatric help, that should involve respect, understanding, empathy or love between humans.

6. Great attention should be given to the immense hazards presented by possible malfunctioning of military command and control systems and autonomous decision-making programs.

7. The Data Protection Act should entitle people to know not only what data are held about them, but also the rules by which they are processed.

8. Statutary regulation of KBS standards may be needed in future.

9. KBS vendors should adopt a suitable Code of Practice.

10. Meanwhile they should be legally obliged to insure themselves against claims for damages by users.

11 Various industry standards are needed, especially in the interface

between the program and the user.

12 Professional associations such as the Society for the Study of Artificial Intelligence and the Simulation of Behaviour, and the Expert Systems Group of the BCS should adopt a code of conduct for their members.

13 Setting up a formal body for KBS practitioners with restricted membership is *not* recommended.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

K Re: Call for Comment, CB "Traffic Advisory Channel" petition

MAINT%UQAM@ugw.utcs.utoronto.ca &eter Jones> Wed, 27 Jun 90 13:53:37 EDT

I am reposting this, after being told that my original postings were only seen on BITNET. Sorry BITNET readers for a possible quadruple posting :-([It has also been posted on SWL-L.]

-----Original message-----

A posting appeared recently on the SWL-L list regarding a computerized information system that informs motorists about traffic conditions:

>Here in Chicago, the Illinois Department of Transportation operates a >group of low-power AM stations that provide traffic information.

>

>The stations broadcast at the top and bottom of the dial (540 and 1610>I think). The broadcast alternates between events affecting traffic>and actual traffic reports. It is all automated.

>

>There is a tape that describes the daily schedule for construction >work, lane closures, ramp closures, parades, and other events >affecting traffic.

>

>This alternates with computerized traffic reports: "As of ... 5:55 pm
>... there is severe congestion on the following currently monitored
>sections of the highway system ... Kennedy expressway ... inbound ...
>between Montrose avenue ... and Irving Park road ... between Kedzie
>avenue ... and the Ohio street junction ..." and so on. The reports
>are updated every 10 minutes or so by sensors buried in the highways.

>

>[text omitted]

>

>One problem with this system is that when traffic comes to a complete >stop somewhere, the computer doesn't detect cars moving over the >sensors and decides that there is no traffic. This is fairly rare. >[text omitted] >

>It's a system that I like a lot.

I find it amusing that this user likes the system, despite its apparently well-known tendency to be completely wrong in worst-case conditions. I wonder if people from out of town are told about this quirk, or left to discover it on their own.

>EMAIL: draughn@iitmax.iit.edu+----+ Academic Computing Center
>BITNET: SYSMARK@IITVAX | Mark Draughn | 10 W. 31st St.
>VOICE: +1 312 567 5962 +----+ Illinois Institute of Technology
>ALSO: ...{nucsrl|att}!iitmax!draughn Chicago, Illinois 60616

New Bank Software => Problems

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Fri, 06 Jul 90 11:12:36 PDT

Today I called my bank (Bank of the West) to transfer some money from one account to another. Before initiating the transfer, I asked for the balance in the source account. The amount the teller said was in my account seemed somewhat high, but in the right ballpark. Since I hadn't balanced my checkbook recently and since it covered the amount I was about to transfer out, I initiated the transfer, thanked the teller, and hung up.

Immediately after getting off the phone, I balanced my checkbook, and realized that the amount she had read to me was about \$2K too high (though the correct amount still covered the transfer). I called back immediately, this time getting a different bank worker. I told her that the amount I had been given earlier was incorrect. She said that the bank had just installed "new software" the previous day, and all account balances were temporarily wrong until "things sort themselves out", which would be a day or so. She said that, unfortunately, not all the bank's employees were aware of the problem.

I wonder what "until things sort themselves out" means. "Until all transactions recorded in the old system are entered into the new one", perhaps? If so, why didn't they do this before putting the new system on-line to workers? Maybe "until bugs in the software are fixed?" If so, their testing of the new software was seriously inadequate.

IJ

Viper and its Formal Verification

Brian Randell &rian.Randell@newcastle.ac.uk> Mon, 9 Jul 90 9:37:15 BST

The RSRE Viper microprocessor and Avra Cohn's report on its formal verification, have been discussed earlier in RISKs. Readers may therefore be interested in the following article, by Simon Hill, which appeared on p.3 of the (UK) Computer Weekly for July 5, 1990. It is reprinted here in its entirety, without permission.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK USER THREATENS COURT ACTION OVER MOD CHIP :: :: :: The first commercial user of the Viper safety-critical chip developed :: by the Ministry of Defence is threatening legal action for alleged :: misrepresentation. :: :: Teknis International Railroad Systems of Adelaide, Australia, is :: seeking assurances that the Viper technology can meet the claims that :: the MoD and its commercial partners make for it. :: :: Teknis, which is developing a signal and railway crossing control :: system using Viper for the Australian National Railway Commission, is :: also threatening action against the MoD's commercial licensee, Charter :: Technologies. :: :: Worcester-based Charter was licensed in january 1988 to exploit :: commercially the fruits of the Viper work carried out at the Royal :: Signals and Radar Establishment at Malvern. :: :: Ron Davison, Teknis' business development manager, says, *We are :: looking for every comfort we can get from the development and :: suppliers of Viper:. :: :: Davison says the A\$12m Australian railways project "is a world first" :: in the safety-critical market, making the first time that Viper has :: found a user outside the military and defence communities. :: :: Teknis' concern has been inspired by a series of reports in UK and US :: academic circles about RSRE and Charter's claims that Viper is :: formally verified for use in safety-critical applications where lives :: may be put at risk if the technology fails. :: :: Davison says he is "surprised at the sudden rash of reports about :: Viper coming out of the woodwork" 18 months after Teknis began work :: with the chip. :: :: But the report that is most critical of Viper, written by Avra Cohn of :: Cambridge University's computer laboratory, is two years old. It was :: published in May 1988 and delivered to RSRE, but Charter technologies :: claims it was not shown Cohn's findings until mid-1989. :: :: RSRE and Charter claim that Viper is formally specified, with a chip :: design which conforms to this specification. Cohn says in the report :: that this is misleading. :: :: "Such assertations, taken as assurances of the impossibility of design :: failure in safety-critical applications, could have catastrophic :: results," Cohn says in the report. :: :: The MoD says "It is a matter of interpretation of the words used to :: describe the dependabiliity of Viper. Nothing can be described as :: absolutely fail safe."

::

:: This year a report by US consultants Computational Logic for US space

:: agency Nasa says "Viper has not been formally verified" and lists four

:: deficiences in RSRE's specification. In a draft copy of the same

- :: report dated June 1989, obtained by Computer Weekly, the former chief
- :: RSRE scientist on the Viper projects, John Cullyer, has indicated his
- :: agreement with Nasa's conclusions. Cullyer is now Professor of
- :: Electronics at Warwick University.

::

- :: The MoD cannot say whether the Nasa and Cohn reports have been looked
- :: at by RSRE staff, but a spokesman says, "Work is continuing to
- :: reinforce verification techniques and if a relevant report has been
- :: produced then it will be studied by scientists at RSRE."
- ::

:: Marconi Electronic Devices of Lincoln, sub-contracted by the MoD to

- :: manufacture Viper hardware circuitry, is reining back on its
- :: commitment to the project while it waits for replies from the MoD.

::

- :: Tony Smith, Marconi Electronic Devices' integrated circuits contract
- :: manager, says the company "wanted a discussion with MoD and RSRE about
- :: what could be guaranteed for Viper. That meeting was due to take
- :: place this year, but the MoD cancelled it. We have still not had that
- :: meeting".
- ::
- :: Marconi has asked the MoD to respond to the Cohn and Nasa reports, but
- :: has not yet received a reply and has not been shown either of the
- :: reports, Smith says. The company is making prototype Viper circuits,
- :: but has no commercial orders.
- ::

:: The Ministry of Defence would not comment on "confidential or

- :: commercial correspondence between it and third parties".
- ::

:: The MoD says, "No Viper chip is known to have failed, but work is

- :: continuing to reinforce and improve verification techniques: on Viper,
- :: and that *although there are not known faults in the Viper design, an
- :: unremitting search for weakness must continue".
- ::
- ::

Cellphone risk to ABS?

Martyn Thomas <mct@praxis.co.uk> Mon, 9 Jul 90 10:01:55 BST

The following appears in an article advising against the use of cellular telephones in aircraft (it's illegal in most countries), published in Flight Safety Bulletin (the quarterly journal of the General Aviation Safety Committee in the UK):

"As a point of interest, the manufacturers of some mobile telephones have issued a warning that they should not be used in cars fitted with an electronic anti-lock braking system (ABS) because the cellphone could cause the system to malfunction."

Presumably the risk is from EMI.

Does any RISKS reader have details on this? Is it just a precautionary warning to limit legal liability, or is there evidence? If this is a real risk, what about coaches, trains, other nearby vehicles ...?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

✓ Car phones and electronic systems

Tim Duncan <timd@aiai.edinburgh.ac.uk> Mon, 9 Jul 90 19:05:01 BST

The following is taken from an article by Kevin Eason in the (London) Times of July 9th:

A safety alert has been issued to thousands of mobile telephone engineers after an incident in which a Jaguar car lost all power because of faulty telephone installation. The driver escaped safely when all electrical systems, including lights, brakes and engine, were shut down by a crossed wire.

Jaguar drivers were warned yesterday to use only car phones fitted and checked by company dealers. The Federation of Communications Services has alerted its 350-member companies which handle mobile communications equipment that faulty installation could damage vital equipment, especially anti-lock braking systems (ABS), and urges them to check with manufacturer specifications.

[...]

The Jaguar driver involved was stranded on a motorway when all power to the car failed. Checks on the vehicle showed that a telephone engineer had crossed vital wires which caused a complete systems shutdown.

Most new cars now have complex computer engine management systems and increasing numbers have electronic controls for suspension, brakes, gearbox and safety mechanisms. The new Mercedes SL convertible sports car, for example, has an automatic pop-up roll bar operated by computer. [...]

Tim Duncan, AI Applications Institute, University of Edinburgh, 80 South Bridge, Edinburgh EH1 1HN, Scotland, United Kingdom. JANET: T.Duncan@uk.ac.edinburgh ARPA: T.Duncan%uk.ac.ed@nsfnet-relay.ac.uk BITNET: T.Duncan%uk.ac.ed@ukacrl.bitnet UUCP: ... mcvax!ukc!ed.ac.uk!T.Duncan

Washington State Ferries slide into home

Joe Dellinger <joe@hanauma.stanford.edu> Tue, 10 Jul 90 00:50:33 PDT

I unfortunately had a Hertz rental car on Orcas Island, Washington, when a Washington State Ferry rammed the Island's only car ferry dock and knocked it out of service for a minimum of several days. The incident raised several interesting points:

1) Hertz had no category for this case; they repeatedly told us "If the car were broken, then you could fly off the island and get another car, and retrieving your car would be our problem. But since you say it isn't BROKEN, every day your car sits on the island is a day you are renting it... and of course if we have to pick it up there you get a retrieval fee, a fee for renting one-way, etc etc".

2) It would be interesting to get more informed information about how the ferries work. From the June 29, 1990 Seattle Times:

From what I could gather from talking to the Seattle Times reporters covering the incident, the ferries have a "fly by wire" propulsion system that among other things does automatic docking. Occasionally the propulsion-control computer hiccups, locking the controls for a few seconds. Normally this is no bid deal, but in this case the computer system had the bad timing to hiccup just as the ferry was supposed to start braking for the final stage of docking at Orcas. As a result the ferry didn't brake at all and ploughed straight into the terminal, causing \$250,000 in damage. (Also costing island merchants much of their July 4 weekend tourist revenue, and severely inconveniencing many unlucky tourists. We eventually managed to get our Hertz car off the island by private barge.)

🗡 Pentagon Pizza

Jim Harkins <jharkins@sagpd1.UUCP> 16 Jul 90 08:48:19 PDT (Mon) Driving to work this morning there was an interesting story on the radio. It seems the Domino's Pizza joint closest to the Pentagon can accurately predict when a major operation is about to take place. Evidently the planning meetings go on long into the night, and the best place to get food is Domino's. They interviewed someone from Domino's and he said that prior to the Panama invasion deliveries to the Pentagon jumped 25%. I'm glad I'm not in security.....

✓ Logica Code Slows Trident

Mark Smith <smith@canon.UUCP> Fri, 20 Jul 90 09:55:34 GMT

This is from the July 19 issue of Computer Weekly:

The 9 billion pound Trident nuclear warhead programme is being held up because of serious problems with a computer system, developed by Logica, that keeps highly volatile nuclear materials apart during weapon assembly.

The system, which ensures the safe movement and records the exact whereabouts of plutonium and other materials around two buildings at the Ministry of Defence's Atomic Weapons Establishment (AWE) at Aldermaston, is only able to handle half the volumes set by the MoD. Despite this, the system went live on July 13.

[...]

The system is a high integrity movement control package, using Stratus fault-tolerant hardware, used in A45 and A90, the two buildings at AWE involved in Trident development work.

One source says that the MoD has set a target for the system to handle 200 units of nuclear material within the two buildings at any one time, but that the present system can only handle 100 units.

The source says that the MoD and AWE have been revising the target downwards, but that Logica has been unable to meet the new figure. [...]

A Logica spokeswoman says it is not company policy to comment on projects which have not been announced.

Yes, this is the same Logica that ran into trouble during a project for San Fransisco's transit system.

Mark Smithsmith@canon.co.ukCanon Research Centre Europe..ukc!uos-ee!canon!smith

✓ GAO slams FAA computer systems

Rodney Hoffman &offman.ElSegundo@Xerox.com> 19 Jul 90 08:02:29 PDT (Thursday)

According to a story by Jeffrey A. Perlman in the 'Los Angeles Times' 18 July 1990, the General Accounting Office has issued a new report entitled "Air Traffic control -- Inadequate Planning Increases Risk of Computer Failures in Los Angeles." The GAO says that in planning for a 1995 consolidation of Southern California radar tracking facilities, FAA officials have refused to consider computer solutions that could solve their computer problems because the agency does not want to rewrite or develop software to run on new, state-of-the-art hardware and expend the "additional time they believe would be required to undertake such an effort."

A 1989 GAO report singled out the Los Angeles - Orange County air space as having the worst comuter-related aircraft tracking problems. The new report criticizes the FAA for ignoring the situation, saying air traffic controllers may find their radar screens flickering, showing insufficient data or blanking out at critical moments.

FAA officials "are still analyzing the GAO report and had no formal reply."

MW Drive-by-wire

Rodney Hoffman &offman.ElSegundo@Xerox.com> 22 Jul 90 11:03:45 PDT (Sunday)

A short item in 'Business Week', July 30:

BMW PUTS A BACKSEAT DRIVER ON A CHIP

The latest cars offer a plethora of computerized wonders -- like chips that control the engine or warn you is a door is ajar. But would anyone want a computer that took over control of a car if it judged the vehicle was being driven too fast or improperly for road conditions? BMW engineers are betting the answer is yes.

They've already installed an early version of their Heading Control system in cars at the auto company's research center in Munich. A camera above the rearview mirror tracks the center stripe and the line along the right side of the road. If a driver gets too close to either marker, a small electric motor integrated into the steering system is activated to put things right. Later versions will gauge road conditions and differentiate between broken and solid lines, so the computer can tell such things as whether it's okay to pass. Drivers being corrected might feel a tug on the wheel. But they can easily override the computer by continuing with wahtever they are doing. BMW engineers say the system is at least five years from market. And they predict that once customers get used to the idea, they'll love it.

Meritish air defense computer suffers a "nervous breakdown"

Walt Thode <thode@nprdc.navy.mil> 19 July 1990 0829-PDT (Thursday)

>From the Reuters news wire:

BRITISH AIR DEFENSE COMPUTER SUFFERING A "NERVOUS BREAKDOWN"

LONDON, Reuter - A nearly half-billion dollar computer designed to mastermind Britain's future air defenses won't be fit for action for another 10 years because of bouts of nervous confusion, Defense Ministry officials said Wednesday.

The \$448.8 million system known as ICCS -- Improved UK Air Defense Ground Environment Command and Control System -- was due to enter service in 1987. But officials told Parliament's defense committee the computer's problems with logic would delay operation by up to 10 years.

"We get wrong answers sometimes and the bugs have to be tracked down and sorted out," Donald Spiers, who heads aircraft control at the ministry, told the committee.

"Secondly, from time to time it crashes. What this means is the equivalent of a nervous breakdown. It becomes confused with the information and goes wrong."

The production consortium, made up of Hughes Aircraft, Marconi and Siemens-Plessey, have upgraded the main computers driving the system to give more power, Spiers said.

ICCS was designed as the sophisticated equivalent of the war tables used during World War II when model planes were pushed around a board.

It will coordinate radar, fighters, surface-to-air missiles and air command centers through a single network.

The system is being developed on a fixed price contract and Spiers said all extra costs had to be met by the consortium.

He said the companies had not been paid for the past two years because of the problems encountered.

--Walt Thode Internet: thode@nprdc.navy.mil UUCP: {everywhere_else}!ucsd!nprdc!thode

Mail signalling software problem

Pete Mellor <pm@cs.city.ac.uk> Mon, 23 Jul 90 20:00:44 PDT

>From the Guardian, Mon. 23rd July, front page:

Headline: BR signalmen 'worked blind'

Subhead: Computer software problems admitted at key commuter train centre

By-line: Patrick Donovan, Transport Editor

British Rail has admitted that computer software problems have been uncovered at a signal centre which controls London's busiest commuter lines. They left operators "working blind" after train movements were wiped off control screens on at least one occasion over the last five weeks.

A BR spokesman said newly installed software, responsible for flashing up the position of trains on the indicator screens of signal operators at Wimbledon,

has been found to contain two technical faults.

The Wimbledon centre controls 90 mph services south of Waterloo and includes the Clapham Junction area, where 35 people died in a train accident in December 1988.

Faulty wiring on a signalling modernisation programme was found to have caused the crash.

BR said one of the faults uncovered on the indicator screen software has not yet been fully rectified. An internal investigation began after an operator found that the system was providing "the wrong information". Realising that he had lost track of train movements, the operator immediately turned all signals to red.

A spokesman said that at no time was any train at risk. "What happened caused concern to the signalman." But he stressed that the mechanical signal equipment and all other equipment worked normally, bringing all trains to an immediate standstill after the problem was discovered.

"The problem was caused by computer software fault in the signal box. [sic - PM] It gave the wrong indication to the signal man. All the trains froze where they were. The lights told him that something was different to what was happening [outside]."

BR conceded that the faulty equipment served a vital function, "this little piece of software tells the signalman what is happening outside".

The software faults were found inside the panel in the train indicator box in a system responsible for operating the lights.

Alastair Wilson, contracts and production director of E. B. Signal, the manufacturers, said: "The system is under test. I do emphasise that things are going through a testing stage. It is not unusual to have minor software bugs." [!!! - PM]

A spokesman for the National Union of Railwaymen said that any operational shutdown of train indicator screens would "at best create a major disruption and at worst could create alarming safety hazards. If everything goes to red it puts enormous pressures on an individual signalman."

[Remainder of article omitted. It goes on about unrelated signalling problems in the Clapham Junction area, including a loss of communication between Waterloo and Wimbledon signal centres, concern about the growing use of driver-only services on Network SouthEast, contradictions in the rule-book about whether or not such services may operate with a defective radio, and the need for the driver to draft competent members of the public to assist him in ensuring safety after an emergency stop.]

A few comments:

The report is rather confused, but it seems that the system receives information about the position of every train in the region, and displays this to the signalmen in the form of lights moving over a large indicator board. The bugs
were in the hardware/software module which drives the display, so it was a case of "correct information in, garbage out".

I wonder if the faulty module was rated as "safety-critical" in the hazard analysis.

It would be nice to know *how* the signalman knew that he was being given wrong information, and what would have happened if he had not been so alert, and continued to operate the network with the wrong information.

It is amusing to hear the manufacturer refer to a bug which brings an entire railway regional network to a standstill for some time as "minor". Perhaps he meant that only a few lines of code were in error! Somebody should have a word with him about how to classify faults and failures!

If, as the manufacturer states, the system is under test, why was it being run to control live traffic without any back-up system? Surely BR's testing strategy can't be "Let the train take the strain"? (To quote one of their own advertising slogans!)

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB Tel.: +44 (0)71-253-4399 Ext. 4162/3/1

Call for Papers on Testing, Analysis and Verification

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Thu, 26 Jul 90 14:39:51 -0700

CALL FOR PAPERS

Symposium on Testing, Analysis and Verification

Victoria, British Columbia, Canada October 8-10, 1991 Sponsored by ACM Sigsoft

The purpose of this meeting is to bring together researchers and practitioners who are working in the areas of software analysis, testing, and formal verification. Papers and panel session proposals are invited on current and emerging techniques, strategies, processes and tools for determining the presence or absence of errors in software and for inferring other characteristics of software quality.

Papers should be a maximum of 5000 words in length. They should present a clear picture of the original contributions made by the paper, while also carefully relating the work presented to the work of others. The highest quality papers from the symposium may be considered for publication in a special issue or section of a research journal.

Authors should send six copies of their paper or panel proposal to the Program Committee Chair, Nancy Leveson, at the address below. Papers must be received by March 1, 1991. Authors will be notified of acceptance by May 15, 1991. Camera-ready papers are due not later than July 1, 1991. **Program Committee** Victor Basili Mark Moriconi Stephen Schach Lori Clarke Mitsura Ohba Gene Spafford K.C. Tai John Gannon Tom Ostrand Susan Gerhart Dewayne Perry Elaine Weyuker Carlo Ghezzi Richard Platek Jack Wileden Richard Hamlet Debra Richardson Bill Young John Knight John Rushby Michal Young For other information concerning the symposium contact: **General Chair Program Chair** Prof. William Howden Prof. Nancy Leveson Computer Science Dept. Computer Science Dept University of California University of California La Jolla, California 92093 Irvine, California 92717 USA USA (619) 534-2723 (714) 856-5517 4 🛖 🕨 🕄 🗹 🗤 🚀 Search RISKS using swish-e Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Sat, 28 Jul 1990 15:18:54 PDT We have had tales of computer-perverted names before. John W. McInroy (Lockheed, Austin) sent me a very cute article by Mike Kelley that appeared in the Austin American-Statesman (23 July 1990, p. A8) describing a computer generated letter recently received by the Austin law firm of Friedman, Weddington and Hansen. Their local bank computer referred to the firm account as "Friedman Wedd etal". This of course led to a letter to Etalfried Wedd from a financial services company, with a "Pre-Approved Loan Authorization" for \$750 requiring only a signature, "because you have demonstrated that you maintain a good credit record ..."

In a wonderful spoof that I will only summarize here, Mike Kelley wrote about "Etalfried" answering indignantly that \$750 "does not justify the time it takes to sign my name", the finance company upping it to \$5,000, another indignant response, then an offer of a loan for \$250,000. The story ends with Etalfried finally getting an unsecured cash loan of \$3.4 billion and retiring to "elegant and commodious surroundings on the sea in a small and remote South American country. ... It is also reported that he takes particular delight in reading over and again the account of how Tom Sawyer contrived to whitewash Aunt Polly's fence." Congratulations to Mike Kelley for spinning a fine yarn.

Pilots vs. automation

<henry@zoo.toronto.edu> Wed, 18 Jul 90 22:13:44 EDT

The 30 May issue of Flight International notes an interesting FAA decision. The latest wonderful innovation for airliners is TCAS, the Traffic alert and Collision Avoidance System, which uses transponder returns from other aircraft to report significant collision hazards and advise the pilots on evasive action. The first TCAS systems are now in airline testing.

The decision says "...enforcement action will not be initiated against flightcrews who deviate from an assigned clearance issued by air traffic control when that deviation is in response to a TCAS-generated resolution advisory and the response is in accordance with the air carrier's approved flight procedures". (A "resolution advisory" is, roughly speaking, a report of imminent danger; TCAS can also issue "traffic advisories", milder warnings of potential trouble, not mentioned in the FAA ruling.)

The airlines and the pilots' union are satisfied with this for now, but would like to see changes to the laws, rather than just a promise not to enforce them, in the long run.

This brings to mind an interesting thought: who gets the blame if (when) a TCAS warning *causes* a collision, through either electronic or human confusion?

Henry Spencer at U of Toronto Zoology utzoo!henry

Widespread use of computer simulations as evidence in court

Jon Jacky <ON@GAFFER.RAD.WASHINGTON.EDU> Tue, 24 Jul 1990 21:57:16 PDT

Here are excerpts from THE SEATTLE TIMES, July 23 1990 p. E3:

COMPUTER ANIMATION AIDING LAWYER'S CASES (from the ORLANDO SENTINEL)

ORLANDO, Fla. --- The truck driver claimed he couldn't avoid hitting and severely injuring the 9-year-old riding a bike. But a one-minute computer simulation depicting the 1986 accident near St. Cloud, Fla., showed that the driver had enough time to miss the rider. The truck driver's insurance company settled the lawsuit in 1988 for \$2.1 million. ...

Whether in depicting auto accidents, plane crashes, industrial accidents or other events, computer animation is fast developing into a powerful legal tool that helps lawyers win cases.

The technology is used primarily by personal injury lawyers who are trying to win big-dollar awards for their clients.

F. Lee Bailey, one of the nation's top trial lawyers, told a group of lawyers at a recent Florida Bar annual meeting in Miami Beach that computer animation is becoming as important as courtroom rhetoric in winning cases.

"There are untold opportunities for the use of animation in the courtroom," said Bob Scott, head of Juris Corp., an Orlando company that produces courtroom exhibits and recently began offering computer animation. "I believe in five years it will be the predominate methodology in showing demonstrative evidence," Scott said.

[There is at least one firm in Seattle that specializes in creating computer animations of accidents for use in court. - JJ]

Jonathan Jacky, University of Washington, Seattle jon@gaffer.rad.washington.edu

✓ Oklahoma computer system foulup

<smb@ulysses.att.com> Mon, 23 Jul 90 23:17:12 EDT

In Oklahoma, about 18,000 state employees were paid late -- very late -because of the cutover to a new computer system. As of today -- 12 days after they should have been paid -- only half of them had received their checks. The state was forced to use an older computer system to write the checks; additionally, since the news story indicates that they had to draw on a special reserve fund, it would seem that the entire disbursement system, and not just the payroll system, is involved.

The problem -- the new code apparently runs too slowly, and input tapes are in the wrong format.

--Steve Bellovin

Mig Brother getting bigger

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Thu, 12 Jul 90 13:54:59 PDT

Excerpted from Gov't Computer News, July 9, p.8:

JUSTICE PROCEEDS TO CREATE ITS DRUG INTELLIGENCE CENTER

The Justice Department plans to spend \$5 million developing systems for its new National Drug Intelligence Center ... [and] about \$55 million to establish the center ... they expect annual operating costs to be about \$27 million. The Justice plan calls for NDIC to become totally operational in 1992 ...

Members of Congress and groups such as Computer Professionals for Social Responsibility and the ACLU have voiced concerns ... they have questioned whether the center might violate privacy laws by using electronic information and linking numerous federal databases into a national database. Thornburgh attempted to quell these fears saying "It's not 'Big Brother'" ... other agencies involved include the the Customs Service, the Coast Guard, the Immigration and Naturalization Service and the FBI. The Defense Department also has assumed increasing responsibility.

An example of the latter is a similarly expensive facility for the Navy, which will integrate data from various radars, besides listening in on telephone calls and so forth.

K RISKS of Publicly-conducted Benchmark Demonstrations

<"Richard_Busch.SD"@Xerox.COM> 13 Jul 90 14:44:41 PDT (Friday)

>From a recent issue of "Computing," the weekly newspaper of the British Computing Society:

"When it comes to choosing a speedy communications channel in today's technology market-place nothing beats a pigeon. Fax company Faxit Europe discovered this to its embarrassment, after pitching one of its high-tech fax machines against Joe, a four-year-old Blue Chequer pigeon.

"The company wanted to show at the launch of its new public pay-fax credit card system that fax is quicker than flight. But they hadn't bargained with Joe, a winner of two open races. Joe beat the fax in a one mile challenge race, arriving more than a minute before the caricature drawing of him emerged from the machine.

"Executives at Faxit Europe were left perhaps not so much with egg on their faces, but with [...] on their collective shoulders."

[Like pigeon pennies? PGN]

✓ Citibank, ATM, electronic transactions

Melik Isbara <isbara@cs.columbia.edu> Fri, 13 Jul 90 02:00:53 GMT

I am posting this article to inform the netters about a problem with Citibank ATM machines and to ask for any information and suggestions. Please bear with me.

When I received my last bank statement, I have noticed three transactions in which \$900 dollars were withdrawn from my accounts from a Citibank ATM machine at a downtown NYC branch which I have never used. (\$900 were withdrawn in three transactions.)

FACTS:

- 1. I did not do those transactions.
- 2. When they took place I was at work out of NYC.
- 3. I did not lose my bankcard or give it to anyone.
- 4. I did not write down my password or tell it to anyone.

After I received my statement I went to my branch and talked to a customer representative. After a couple of days I got two letters from Citibank saying that results of their investigation (which consists only of looking at the ATM machine records for those specific transactions) showed that for those transactions my bankcard and my password were used therefore they could not honor my claim.

Now my guess is that this is most probably a software problem because last weekend I went to the branch where money was withdrawn and there was a sign on the door saying that the ATM machines there were out of order. I also learned that they have been out of order for about a week.

I am going to take a legal action against to Citibank therefore I would like to know if anybody is aware of a similar situation or if anyone has any ideas on how this might have happened. I would appreciate any information and suggestions that can help me to fight Citibank to recover my money and to explain how this event might have happened.

Please e-mail to mii@briar.philips.com or isbara@cs.columbia.edu Thanks in advance.

Melik Isbara, Columbia University, Dept. of Electrical Eng.

Disclaimer: My employer is not responsible for the content of the article posted above.

✓ USAF ECM systems: software 2 years late

Martyn Thomas <mct@praxis.co.uk> Tue, 31 Jul 90 14:37:43 BST According to Flight International (25-31 July 1990, p13), the US General Accounting Office has discovered that the Westinghouse electronic countermeasures (ALQ-131 jammer) on F16s and F111s in Europe are inoperative because the "no suitable software had been supplied" for the "Loral receiver-processor", two years after delivery.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

A320 FADEC Software Diversity??

Pete Mellor <pm@cs.city.ac.uk> Fri, 22 Jun 90 22:36:18 PDT

The Electronic Flight Control System (EFCS) is not the only flight-critical software controlled system on the A320. The Full Authority Digital Engine Control (FADEC) is another.

Single points of failure of hardware can be eliminated from system design by using redundant components or hardware subsystems. To achieve a similar design aim where software is concerned requires diversity. The EFCS in fact incorporates both software diversity, hardware design diversity, and hardware redundancy. See, for example:

Traverse P.J.: "Dependability of Digital Computers on board Airplanes"
 Preprints of 'Dependable Computing for Critical Applications',
 IFIP WG 10.4 Intl. Working Conference, Santa Barbara, CA, Aug.1989,
 pp 53-60

I have recently received copies of:

Cosimo J. Bosco: "Certification Issues for Electrical and/or Electronic Engine Controls." SAE Technical Paper Series #871844, 1987 Keywords: EEC electronic engine controls FADEC certification issues

and:

Federal Register Vol. 54, No. 17, Jan.27, 1989, Docket No. NM-26: "Special Conditions: Airbus Industrie Model A320 Series Airplane." (Final special conditions for certification)

Bosco states (p. 20) that "The all electronic FADEC is usually a completely redundant, dual-channel, primary/secondary type of system. Current systems have successfully employed *ESSENTIALLY THE SAME SOFTWARE* in each of the redundant channels." [my emphasis]

Now, if the same software is loaded into redundant hardware processors, any bug is a potential source of single-point failure of the system as a whole. Bosco in fact goes on to discuss this very point.

The final special conditions in docket NM-26 do not require diversity as such,

only that "...the components of the propulsion control system...must have the level of integrity and reliability of a hydromechanical system (HMC) meeting current airworthiness standards".

In the discussion printed below this statement of the requirement, it is stated that in practice this "...is demonstrated by an inservice loss of thrust control approximately once per 100,000 hours of operation...This level of reliability for the loss of thrust control on one engine will result in an overall airplane propulsion control system reliability that is consistent with the guidance [presumably 10^-9 probability of failure as in AC 25.1309-1] associated with 25.1309(b)(1), *ASSUMING AN INDEPENDENCE OF THE FAILURE CONDITIONS THAT CONTRIBUTE TO THE LOSS OF THRUST CONTROL*."[my emphasis again]

The question that I ask is therefore: "Does the FADEC as *actually* certified on the A320 employ diverse software in the different channels?".

My suspicion is that the FADEC does not incorporate dissimilar software, and that its software can therefore be a source of common mode failure for the whole propulsion control system. This would seem to contradict the special condition referred to above. At the same time, the FAA seems to be very well aware of the common mode failure potential of software.

Even if the same two dissimilar programs are present in both FADECs, it is possible for a bug in one homologue to be a common point of failure between the two engines.

FADECs are relatively mature devices. Does anyone out there have any hard information, particularly references to published papers?

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V OHB Tel.: +44 (0)71-253-4399 Ext. 4162/3/1

Hubble problems

Eugene N. Miya <eugene@wilbur.nas.nasa.gov> Sun, 1 Jul 90 17:29:26 -0700

"Ain't hindsight wonderful?"

First off, any large complex project is bound to have problems. I'm not saying that I support my employer or defend the HST. Consider for instance that other institutions are also bound to have used some of the same types of components in their systems: Perkin-Elmer (and its subsidary), Lockheed, etc. are all going to feel this (in one investigation which JPL was involved, LMSC was also blasted by Congress). P-E is making mirrors and instruments for other projects, I would worry about Keck for instance.

Second, every project is a set of compromises. I've have seen other criticisms of HST in the science press before launch and also had my own criticisms of GSFC. Those of "us" who have been on "losing teams" aren't off saying "I told you so." But in finger pointing, it does not help to keep wheat and chaff together. The less noise when trying to locate problems, the better.

Lastly, it is important to note this isn't bad just for NASA but bad for big science and science projects in general. I worry about the "climate" for any research in this country, because research tends to fail 90% of the time (if you really need a reference for this I have it). The next time, it might not be a satellite telescope, but maybe a particle accelerator, a computer project, or who knows. Are we are too involved in finger-pointing and not enough involved to 1) help fix, 2) stay out of the way of those trying to fix (keeping quiet unless we have significant info)? Are we contributing to the demise of any research funding (DARPA, NSF, NASA, DOE as well as private) at all?

e. nobuo miya, NASA Ames Research Center, eugene@orville.nas.nasa.gov {uunet,mailrus,other gateways}!ames!eugene

🗡 Re: Pentagon Pizza

<henry@zoo.toronto.edu> Mon, 30 Jul 90 12:28:23 EDT

>interviewed someone from Domino's and he said that prior to the Panama invasion>deliveries to the Pentagon jumped 25%. ...

This sort of thing is not new. During WW2, John Campbell -- editor of Astounding Science Fiction and essentially the founder of modern SF -apparently had a wall map with colored pins showing the distribution of A.S.F. sales. He found it interesting that A.S.F. sold many copies in obscure places like Oak Ridge and Los Alamos, where there wasn't supposed to be anything noteworthy going on...

Henry Spencer at U of Toronto Zoology utzoo!henry

🗡 CTS info requested

<wex@pws.bull.com> Wed, 18 Jul 90 12:30:43 edt

Recently, several informative articles on Carpal Tunnel Syndrome (CTS) appeared in RISKS. I would like to correspond with any RISKS readers who have first-hand experience with the condition and its treatment.

Please write or call me.

--Alan Wexelblat Bull Worldwide Information Systems internet: wex@pws.bull.com phone: (508) 294-7485 (new #) Usenet: spdcc.com!know!wex

More on carpal tunnel syndrome/RSI

Chrome Cboy <sobiloff@agnes.acc.stolaf.edu> Thu, 12 Jul 90 09:19:38 CDT >Date: Thu, 28 Jun 90 14:11:52 EDT
>From: henry@zoo.toronto.edu
>Subject: Re: info on carpal tunnel syndrome (CTS)

Henry Spencer asks:

>What was the incidence of CTS twenty years ago, when electric typewriters >routinely had non-linear force-depression curves? Or before that, when >manual typewriters required far more finger pressure than any modern >keyboard? Yet again, we have here a case of a "computer risk" that isn't >really new, and data from olden days could be very useful in deciding what >*really* causes it.

Unfortunately I don't know of any data that is available concerning RSI in typists before the introduction of computers to the work environemnt. However, what Henry is overlooking is how a typist's job has changed with the advent of computers. Instead of having to pause every page to change the paper, and in some cases at the end of every line to return the carriage, now a person can sit at a computer uninterrupted for hours on end. This greatly increases the amount of stress on the carpal tunnel because there is very little variance in movement any more.

I agree that it would be nice if there were data from the "olden days" that details typists, but all the data I am aware of (which isn't much) deals with RSI in factory workers. I wish I could interpret this as meaning that RSI was not prominent enough to garner any attention, but that would be overextending the data (or lack thereof).

Also, RISKS readers might want to familiarize themselves (if they aren't already) with the RSI problems in Australia. This is a very interesting situation where the incidence of RSI is very high, but there is some data that suggests that the explosion of RSI cases may have more to do with unsatisfactory work conditions (pay, not posture) and the health-care system's treatment of RSI than with actual physical problems. I'm afraid I don't have any references handy, but I could provide them in short order if anyone wishes to pursue this further.

Blake Sobiloff, St. Olaf College

Kisk Management in the public sector (Request for info)

Mark A. Yedinak <yedinak@motcid.UUCP> 17 Jul 90 14:26:12 GMT

I am posting this for my father, who is looking for text on the subject of Risk Management within the public sector. He is interested in automating a materials handling system and would like information on the risks associated with automation of similar systems. He would also be interested in any other significant articles relating to risk within the material control and financial management areas. Email can be sent to me directorly at the below address or to him via US Mail or fax at:

Mike Yedinak, Chicago Transit Authority Merchandise Mart Plaza Room 725 Chicago, IL 60654 Fax: 312-763-6369 Thanks for the assistance. Mark A. Yedinak, Motorola - General Systems Sector, 3205 Wilke Road, Arlington Heights, IL 60004 708-632-2874 - uunet!motcid!yedinak equal to the maintainerReport problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Wed, 1 Aug 1990 17:39:32 PDT

New York Woman (presumably the current issue) addresses a problem common to women (and men) in the Big Apple: roaches in your personal computer. The recommended solutions include traplike surrounds, replacing oxygen with carbon dioxide in an airtight container (with the computer OFF), spiders (even if you have aRACFhnophobia?), or find a specialist to take it apart and "administer a nice, roach-repelling pesticide." Also included are disrecommendations, such as not enclosing it in an airtight plastic container with the power on, and not putting it in the fridge. [Source: San Francisco Chronicle, 1 August 1990, p.

A10.]

RISKS has dealt with all sorts of bugs, but I don't recall mention of roaches in our five-year roadshow (roach-ho!). Oh, yes, 1 August 1990 marks the FIFTH ANNIVERSARY OF THE VERY FIRST RISKS ISSUE. This is our 774th issue, averaging about 3 a week through thick and thin. Sheer heroism on the part of your moderator? Or masochism? Either way, its been fun (except for the mailer headaches).

So, let me take this opportunity to report on sendmail bugs. We installed a patch that deletes from the in-progress list any address for which successful mailing appears to have been accomplished. A few of the addresses on one of the sublists (but not consecutive ones) still managed to get multiple copies of RISKS-10.16, one of the copies bearing a botched (incomplete) last line of the header routing information. This looks like a NEW bug, so we have backed off to the old mailer for a while longer -- because it had seemingly been reliable lately. At this point I'm ready to try the plastic bag approach. I know that pesticides don't provide a very sound solution, ecologically or otherwise. PGN

BMW's 'autopilot'

<"Richard_Busch.SD"@Xerox.COM> 31 Jul 90 10:33:32 PDT (Tuesday)

In <u>RISKS-10.15</u> Rodney Hoffman quotes from 'Business Week', 30 July 1990:

>[BMW have]already installed an early version of their Heading Control system in cars...A camera above the rearview mirror tracks the center stripe and the line along the right side of the road. If a driver gets too close to either marker, a small electric motor integrated into the steering system is activated...Later versions will gauge road conditions...<[etc.]

There are two possible problems here. Assuming (as one has no right whatever to do) that the system as implemented is technically perfect and never fails, one is still left with some difficulties to do with the nature of driving:

1. If, as it would seem, the system relies on the uniformity of the road construction then it will be unable to work on roads other than motorways (freeways, autobahnen, autostrada, etc.) which are of modern construction and uniform design. It will definitely not work in many urban or suburban areas in which roads are usually far from uniform. It is on such roads (probably for similar reasons) that most accidents occur. Motorways have very low accident rates per vehicle-mile. It is therefore odd seemingly to address only the problem of course loss (often due to sleep) on otherwise rather safe roads.

2. Even if the course loss problem were the main concern, then without some method of detecting a vehicle ahead and slowing or stopping the guided vehicle automatically, the system seems likely to ensure that a sleeping driver will be unerringly guided into a nose-to-tail collision with the first slower-moving vehicle encountered in the same lane.

3. The decision to overtake is prompted not primarily by the absolute legality

of the operation (i.e. over which type of line one proposes to pass), but by the view of the road ahead, which is not available to this system. A mechanical veto on overtaking, particularly taking the form of a 'twitch' of the steering at the critical moment when the front wheel crosses the line, seems almost certain to bring about accidents. The system could not reasonably be expected to distinguish between the solid line in the centre of a minor road, which one may not cross, and the solid line around the edge of the warning zone at the junction of a motorway and its sliproad, which line one may cross in emergency. It could thus intervene at a critical moment during an emergency; hardly a contribution to road safety.

4. The experience of the introduction of ABS strongly suggests that if the system is installed then it will be systematically abused. ABS appears to encourage some drivers both to take unreasonable risks of loss-of-control accidents, and to demonstrate their 'machismo' by charging the last vehicle in a stationary queue, making an 'ABS stop' at the last moment. The introduction of BMW HCS would infallibly bring about a perception on the part of such people that they can (a) use as many handheld telephones as they wish; (b) read the newspaper while driving; (c) drink more alcohol before attempting to drive, since the car can 'find its own way home'.

In my view this development and many like it are fatuous, and are not an acceptable substitute for responsibility on the part of drivers. Expecting people (indeed, allowing them to be encouraged) to behave competitively and aggressively on the road and then proposing by technical means to prevent them from causing accidents are not the correct solution to a high accident rate.

Chaz

🗡 SIGSOFT '91

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 31 Jul 1990 10:56:01 PDT

PRELIMINARY ANNOUNCEMENT

SIGSOFT '91: Conference on Software for Critical Systems

Location: Washington, D.C. area Dates: 10-12 December, 1991

General Chair:

Mark Moriconi, SRI International (moriconi@csl.sri.com) Program Co-Chairs: Nancy Leveson, UC Irvine (leveson@ics.uci.edu) Peter Neumann, SRI International (neumann@csl.sri.com)

Computers are being introduced into systems that affect nearly every aspect of our lives. There are very good reasons to do so ranging from economics to efficiency to enhancing effectiveness and capability. But in the enthusiasm to take advantage of computer capabilities, we are becoming increasingly vulnerable to errors and deficiencies in the software. The SIGSOFT '91 Conference will provide a forum in which research on all aspects of quality in critical systems can be presented. A critical system is a system that must exhibit, with very high assurance, some specific qualities such as safety, reliability, confidentiality, integrity, availability, trustworthiness, and correctness. The conference will focus on architectures, design methodologies, languages, analysis techniques, processes, and experience that can increase the likelihood that a system exhibits its required qualities.

Papers will be due in the Spring of 1991. More details will follow. Please save the dates.

Program of the European Symposium on Research in Computer Security

ESORICS-90

<deswarte@tsf.laas.fr> Mon, 16 Jul 90 10:32:04 +0200

EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY October 24-26, 1990, Toulouse, FRANCE

The aim of this symposium is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas. To achieve this aim in the best conditions, ESORICS-90 will be a single track symposium and the selected papers will be presented in a conference hall whose capacity is 250 attendees.

Computer security is concerned with the protection of information in environments where there is a possibility of intrusions or malicious actions.

* HONORARY CHAIRMAN GILLES MARTIN (deceased on February 7, 1990)

- * CHAIR AND PROGRAMME CHAIR Gerard Eizenberg, ONERA/CERT
- * ORGANIZATION CHAIR Marie-France Kalogera, AFCET
- * LOCAL ARRANGEMENTS Brigitte Giacomi, Ghyslaine Picchi, ONERA/CERT
- * ORGANIZED BY AFCET, IN COOPERATION WITH

AICA Associazione Italiana per l'Informatica ed il Calcolo Automatico
BCS The British Computer Society
ESA European Space Agency
GI Gesellschaft fur Informatik
IEEE-CS The IEEE Computer Society
DISSI Delegation Interministerielle pour la Securite des Systemes d'Information
DRET Direction des Recherches Etudes et Techniques
FRANCE TELECOM
INRIA Institut National de Recherche en Informatique et Automatique
TECHNICAL PROGRAMIME

WEDNESDAY, OCTOBER 24, 1990

8:30 Registration 9:40-10:00 Welcome and Introduction 10:00-11:00 Database I, Robert Demolombe, Chair Teresa F. Lunt, Donovan Hsieh - "The SeaView Secure Database System: A Progress Report" Kioumars Yazdanian - "Relational Database Granularity" 11:30-12:30 Database II, Teresa F. Lunt, Chair Udo Kelter - "Group-Oriented Discretionary Access Controls for Distributed Structurally Object-Oriented Database Systems" Joachim Biskup - "A General Framework for Database Security" 2:00-3:30 Secure Systems I, Dennis Steinauer, Chair R. W. Jones - "A General Mechanism for Access Control: Its Relationship to Secure System Concepts" Jorg Kaiser - "An Object-Oriented Architecture to Support System Reliability and Security" Zoran Savic, M. Komocar - "Security Kernel Design and Implementation in the IBM PC Environment" 4:00-6:00 Secure Systems II, David Bailey, Chair G. Hoffmann, S. Lechner, M. Leclerc, F. Steiner - "Authentification and Access Control in a Distributed System" I. Akyildiz, G. Benson - "A Security Level Reclassifier for a Local Area Network" Laurent Blain, Yves Deswarte - "An Intrusion-tolerant security server for an open distributed system" E. Stewart Lee, Brian Thomson, Peter I. P. Boulton, Michael Stumm -"An Architecture for a Trusted Network" 6:15 Poster Sessions THURSDAY, OCTOBER 25, 1990 9:00-10:30 Models I, Franz-Peter Heider, Chair Brian Thomson, E. S. Lee, P. I. P. Boulton, M. Stumm, D. M. Lewis - "Using Deducibility in Secure Network Modelling" Vijay Varadharajan - "A Petri Net Framework for Modelling Information Flow Security Policies"

Anas Tarah, Christian Huitema - "CHIMAERA : A Network Security Model"

11:00-12:00 Models II, Luis Farinas del Cerro, Chair

Frederic Cuppens - "An epistemic and Deontic Logic for Reasoning about Computer security"

Colin O'Halloran - "A calculus for information flow"

1:30-3:00 Cryptography, Louis Guillou, Chair

D. de Waleffe, J.-J. Quisquater - "Better login protocols for computer networks"

Marc Girault, Jean-Claude Pailles - "An Identity-Based Scheme Providing Zero-Knowledge Authentication and Authenticated Key-Exchange"

Jacques Patarin - "Generateurs de permutations pseudo-aleatoires bases sur le schema du DES"

3:30-5:00 Panel : "Update on Public-Key know-how", Paul Camion, Chair

5:15 Poster Sessions

FRIDAY, OCTOBER 26, 1990

9:00-10:00 Software Engineering for Security, Rene Jacquart, Chair

E. S. Hocking, J. A. McDermid - "Towards an Object Oriented Development Environment for Secure Applications"

G. P. Randell - "A Case Study in the Formal Refinement of a Distributed Secure System"

10:30-11:30 Security Verification and Evaluation, Peter Bottomley, Chair

Pierre Bieber - "Epistemic Verification of Cryptographic Protocols"

Eric Deberdt, Sylvain Martin - "Methodologie "Minerve Securite": Demarche d'Evaluation de la Securite des Logiciels"

11:30-12:30 Panel : "Security in Software Developments Environments" Chris Sennett, Chair

2:00-2:45 David Bailey (invited) - "Managing Computing Security: What is Needed from the Research Community?"

2:45-3:15 Jean-Francois Pacault (invited) - "Harmonizing the Information Technology Evaluation Criteria"

3:45-5:15 Panel : "Impacts of Evaluation Criteria on Research" Christian Jahl, Chair

5:15-5:30 Closing Remarks

SYMPOSIUM LOCATION : F.I.A.S. (Formation Internationale Aeronautique et Spatiale) - 23, avenue Edouard-Belin - 31400 Toulouse - France telephone : +33 61 55 00 87 - telefax : +33 61 55 16 97

CONTACTS: For other general information concerning the symposium, contact : Veronique SEGAUD - AFCET - tel : +33 1 47 66 24 19, fax : +33 1 42 67 93 12

[Full registration information and application form can be obtained on-line from deswarte@tsf.laas.fr or from risks-request@csl.sri.com, or FTPed from the CRVAX.SRI.COM machine (see masthead instructions) with file name "conf.esorics". PGN]

Pilots vs. automation (Henry Spencer, <u>RISKS DIGEST 10.16</u>)

Bob Sutterfield <bob@MorningStar.Com> Wed, 1 Aug 90 17:13:38 GMT

This isn't a promise not to enforce the laws, it's a fairly straightforward interpretation of some of the most fundamental aviation regulations in existence (and long-standing, harking back to days of captains on the high seas, out of touch with their admiralties for months running).

By U.S. Federal Aviation Regulation 91.3(b), "In an in-flight emergency requiring immediate action [such as a TCAS alert], the pilot in command may deviate from any rule of this part [including clearances] to the extent required to meet that emergency." I suspect that the ALPA's beef is that they'd just like it more explicitly worded with respect to TCAS and other automated aids, and perhaps changed to "a perceived in-flight emergency."

This brings to mind an interesting thought: who gets the blame if (when) a TCAS warning *causes* a collision, through either electronic or human confusion?

By FAR 91.3(a), "The pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft." If Air Traffic Control instructs a pilot to fly into the side of a mountain, the pilot is at fault if he follows along. If TCAS says "CLIMB!" it's still the pilot's responsibility to decide whether to obey. It's the pilot's job not to be confused.

General aviation pilots have voiced the concern that TCAS will lead to complacency on the part of air carrier crews, depending too much on the technology, leading to a breakdown of the basic "see and avoid" (FAR 91.113(b)) means of avoiding collisions, which is still the only method that will work when flying near non-transponder-equipped aircraft. Air carrier pilots respond, as expected, that everyone should have a transponder. And so it goes...

Altitude violations and TCAS

<ark@research.att.com> Wed, 1 Aug 90 10:21:45 EDT

It's not clear that deviating from a clearance is violating the regulations at all. My evidence:

From the Pilot/Controller Glossary:

Emergency: a Distress or Urgency condition

Distress: A condition of being threatened by serious and/or imminent danger and of requiring immediate assistance

Urgency: A condition of being concerned about safety, and of requiring timely but not immediate assistance; a potential Distress condition.

So, if your TCAS has just told you that you might hit another airplane if yuo don't change course, that's an emergency.

Now we turn to Federal Aviation Regulations, Part 91: General Operating and Flight Rules. Section 91.123 is where it says you can't leave an assigned altitude:

(a) When an ATC clearance has been obtained, no pilot in command may deviate from that clearance, except in an emergency....

(b) Except in an emergency, no person may operate an aircraft contrary to an ATC instruction in an area in which air traffic control is exercised.

(c) Each pilot in command who, in an emergency, deviates from an ATC clearance or instruction shall notify ATC of that deviation as soon as possible.

And section 91.3 gives blanket authorization:

(a) The pilot in command of an aircraft is directly responsible for, and is the final authoriaty as to, the operation of that aircraft.

(b) In an in-flight emergency requiring immediate action, the pilot in command may deviate from any rule of this part to the extent required to meet that emergency.

(c) Each pilot in command who deviates from a rule under paragraph (b) of this section shall, upon the request of the Administrator, send a written report of that deviation to the Administrator.

This seems pretty clear. A pilot who realizes the possibility of a midair

collision has the authority and responsibility to do whatever is necessary to prevent it. After deviating from course one must notify ATC (``New York Center, Cessna 5-7-Tango turning right 2-0 degrees to avoid traffic'') and file a written report if requested, but emergency deviations are explicitly allowed by the regulations.

Andrew Koenig (private pilot, instrument airplane single-engine land)

Risks of Research vs Errors

Dave Davis <davis@mwunix.mitre.org> Wed, 01 Aug 90 09:55:25 EDT

In the 10.16 edition of Risks, Mr. Miya points out that about 90% of research fails. However, the Hubble telescope's problems are a bit more mundane, NASA just goofed. When a research experiment fails to give us the answers we expected, we must adjust our theory and possibly our hypothsis and begin again. Hubble's problems indicate to many in Congress as well as the public that NASA has problems managing itself as well as its contractors. Ironically, it seems that a part of the difficulty stems from the use of a notoriously secretive Air Force affiliated contractor to do the critical mirrors.

Dave Davis, MITRE Corporation, 7525 Colshire Dr., McLean, VA 22102

🗡 Re: Hubble Trouble

Brinton Cooper <abc@BRL.MIL> Tue, 31 Jul 90 22:53:42 EDT

RE Gene Miya's "hindsight" arguments:

I agree that complex projects have "problems" and that many (not "every") projects involve "compromises." These are EXACTLY the reasons for ADEQUATE and THOROUGH TESTING. The lack of testing and the fuzzy-headed thinking that rationalized away the need for testing are nothing new to observers of the DoD (MY employer, folks). Our systems have been failing for years because of inadequate independent testing and evaluation.

I wonder if there's a connection between NASA's increasingly poor performance and the increasingly large number of ex-DoD types working there in VERY high places?

"Lastly," we all agree that much "research" ends in "failure" according to the uninformed definition of "success." But building the Hubble was no research project. It was an ENGINEERING job.

Needless to say, these opinions are mine and do not constitute an official Army position, etc, etc.

Brint

Hubble Trouble (Mirror, mirror, on the wall)

Bryce Nesbitt <bryce@cbmvax.cbm.commodore.com> Wed, 1 Aug 90 00:21:13 EDT

Eugene N. Miya <eugene@wilbur.nas.nasa.gov> writes: >I worry about the "climate" for any >research in this country, because research tends to fail 90% of the time (if >you really need a reference for this I have it).... >[Perkin-Elmer] is making mirrors and equipment for other project, I would >worry about Keck for instance.

I agree with your point about research, but I view Hubble as "screwed up research" instead of "a good try that failed". The mirror was only the latest serious screwup. I have no inside track on Hubble; that's just an outside impression.

The Keck mirrors have been a concern. There is a difference from Hubble, however. Keck uses asymmetrical mirror segments. Each of the 36 segments is a slice of the final shape. Weights are hung from each segment, the mirror is conventionally ground, then the weights are released. All this is very new, and very research oriented. (Perkin-Elmer is not involved, unless it happens to own Itek, the primary mirror contractor).

Hubble's mirrors are precise, but nothing special. I find it ironic to go back to some glowing magazine articles about how well the the mirrors were built... they exceeded spec on several points (including reflectivity). The builders seemed very proud.

RISKS of slanting computer related excerpts

"Jay Schmidgall" <shmdgljd@rchvmw3.iinus1.ibm.com> Wed, 1 Aug 90 08:38:26 CDT

In a recent digest, "Richard_Busch.SD"@Xerox.COM writes

- > [...] Joe, a four-year-old Blue Chequer pigeon.
- >
- > [...] Joe beat the fax in a one mile challenge race, arriving more
- > than a minute before the caricature drawing of him emerged from the
- > machine.

It should be noted that the pigeon was given a two-minute head start before the fax company began its transmission. As I read the actual article, it appeared that the pigeon had arrived before the company even began it transmission.

While we all may enjoy that good old-fashioned methods can sometimes subvert the best efforts of modern technology, we should not let this be portrayed in unrealistic examples. The referenced excerpt made it sound



Koller Coasters scarier - but safer - than ever (???????)

Bob Felderman <feldy@CS.UCLA.EDU> Fri, 3 Aug 90 00:22:47 -0700

Excerpted from TIME magazine August 6, 1990

Two risks I noticed in the article:

In regards to the design of the coasters:

To achieve these extremes, designers create computer-simulation models that show the effects of high speed and sudden force on the riders, the cars and the structure. This enables the engineers to build roller coasters with the steepest possible inclines and most sharply banked curves to create the illusion of breakneck speed.

Regarding the operation of the coasters:

Most rides are directed by two sets of programmed logic controllers encased in small bunker-like rooms beneath the stations where the riders board the cars. The computers monitor the distances between trains by means of solid-state sensors embedded in the rails. If a train slows or stops, others behind it are halted. Multiple sets of pneumatic brakes can automatically slow a train down midway through a course. By allowing the new coasters to run three of more trains at the same time (as opposed to one on the old rides), the electronics have boosted rider capacity from an average of 500 people an hour to more than 2,000.

Park operators say the technology has also improved safety. Some coasters, like nuclear-missile launchers, require two attendants, pushing separate buttons, to dispatch a train. [text deleted]

Operator error has been eliminated," asserts Richard Kinzel, president of Ohio's Cedar Point park. Says Paul Ruben, editor of "RollerCoaster!" magazine: "If people really knew how safe they are, roller coasters would lose a lot of their thrill."

Bob Felderman, UCLA Computer Science!{rutgers,ucbvax}!cs.ucla.edu!feldy

Kisks of de facto standards

Michael L. Littman <mlittman@breeze.bellcore.com> Sat, 4 Aug 90 08:47:01 -0400

Richard Stallman of the Free Software Foundation (the GNU folks) recently announced on the gnu.announce mailing list that the Lempel-Ziv-Welch algorithm on which "compress", "uncompress", and "zcat" may be covered by a patent assigned to Unisys. Unisys claims that people should not be running these programs without their permission.

Since "compress" is the de facto standard method for moving big files across the net cheaply (and I believe for high speed modems as well), this could create some serious problems. For one thing, if people stop using compress it could really put a strain on the network.

On the other hand, sending people compressed files could put them in the potentially legally precarious position of running uncompress without permission. This is the position the GNU folks seem to be taking. They will either find a new data compression algorithm or send around uncompressed files (as soon as they can find the disk space to store the uncompressed tar files!)

If the POSIX committee is not able to license the algorithm, they will drop these utilities from the next draft of the standards (according to a draft of the POSIX user portability extension standard P1003.2a).

Depending on your political orientation, this can be viewed as a RISK of software patents or a RISK of dependence on a de facto standard. In either case, life may be a little tougher without "compress".

Michael L. Littman [MRE 2L-331 x-5155] mlittman@breeze.bellcore.com

***** Re: 90% of research experiments fail, Risks of Statistics

Jeremy Grodberg <jgro@apldbio.com> 3 Aug 90 04:31:07 GMT

In <u>Risks 10.16</u>, Eugene N. Miya <eugene@wilbur.nas.nasa.gov> claims that 90% of research experiments fail. I trust he is using a different definition of failure than most scientists.

An experiment is a test designed to discover something not yet known. An experiment fails only when nothing is learned. It is usually (some would say definitively) the result of improper design of the experiment.

It is a matter of lore that Thomas Edison tried over 1000 different materials for making light bulb filiments before finding tungsten. I view that (as I believe most scientists would) as 1000 successful experiments, 999 showing that certain materials won't work, and probably giving some indication as to why. I expect the 90% failure rate Mr. Miya speaks of is from the point of view that this was 999 failures and 1 success. I also suspect that this figure was more or less invented ("estimated" is the conventional euphemism) by someone, although probably not Mr. Miya.

The Hubble (which is what started all this) is a (partial) failure because its mirror problems are keeping parts of the telescope from providing anything useful; it is not discovering anything not previously known. This is quite different from having a perfect Hubble showing us that the view from up there looks exactly like the view from down here; that would be very surprising and educational indeed!

Improper use of statistics is one of the greatest problems we face today. Most often, their use is misleading just as in this example, where vague terms obscure the actual meaning of the statistic. If 90% of government funded experiments fail (as I take the meaning of failure), this is a very serious problem calling for overhaul of the whole government funding system. If, however, the 90% just don't yield the hoped for outcome, who cares?

Some anti-abortionists claim they have surveys indicating a vast majority of Americans "support some restrictions on abortion." This could conceivably mean that most Americans feel that women should have to wait at least 4 hours between the time they ask for an abortion and the time it is performed, to give them a chance to change their mind. Obviously the intent is to make people think that most people are opposed to people having abortions. Please no flames on abortion politics, this is just about the statistical claim, which I believe was made to support AT&T's decision to withdraw its support from Planned Parenthood.

I wish there were some way we could reduce the risks to society of statistics. We have drug testing, sobriety checkpoints, tax systems, and all sorts of other government programs which are sold to the public on the basis of just such statistics. A recent Scientific American article refuted the claim that mandatory testing of employees for drugs is beneficial, by reexamining the studies and what their results can show; these results were often used in a misleading way by citing only some statistical findings. Other researchers have determined that there is no sound basis for the cholesterol-lowering treatment regimens many people are put on to reduce the risk of heart attack; the studies indicate a correlation between high cholesterol and risk of heart attack, but do not show that lowering cholesterol by the amounts normally achieved with "conventional" treatment have *any* effect on heart disease. (There is a brand new study which shows some beneficial effects of a comprehensive therapy which reduces cholesterol among other benefits, but that study reduces cholesterol much more than "conventional" therapies, and they do not even claim that the cholesterol reductions are the reason for the therapies success, since some people in the study had very high levels even after the reduction.)

So be very skeptical of statistics, and try to find a solution to this problem. Meanwhile remember, as some net-person reminds us in his signature,

97.43% of all statistics are made up.

Jeremy Grodberg

Ke: British Rail signalling software problem

Clive Feather <clive@x.co.uk> Tue, 7 Aug 90 06:40:54 bst

In <u>Risks 10.15</u> Peter Mellor quotes an article from the Guardian about signalling problems in British Rail.

I would like to add a few comments on this material lest Risks readers get the wrong ideas.

>From the descriptions in the article, and from memory, the area is fitted with what is known as an NX signalling system with a VDU and tracker-ball based user interface. These systems consists of two independent parts - the interlocking and the control system.

The interlocking is relay based circuitry which actually controls points and signals. In computer terms, its input are push buttons and hardware train detectors (usually track circuits, which detect trains because they connect the rails together electrically), and its outputs are signal lamps, points motors settings, and display lamps.

The interlocking is a safety-critical system, and is designed accordingly. The system must be proof, for example, against any combination of relays failing normally, and against an earth fault at any single point. It is the responsibility of the interlocking to ensure that two trains cannot be signalled on colliding paths, for example.

> A BR spokesman said newly installed software, responsible for flashing up the> position of trains on the indicator screens of signal operators at Wimbledon,

> has been found to contain two technical faults.

In older installations, the push buttons and display lamps mentioned above are physically present; a route is set for a train by pressing two buttons, and a train's presence is indicated by a magenta light. In newer systems, including I believe the one in question, the displays and controls are computer and VDU based. The display system is *not* safety critical, as any malfunction can only cause bad commands to be sent to the interlocking.

A third part is the train identification system. This takes information from the interlocking and from manual input, and displays train identities on the control panel or screen. It has no input back to the interlocking, and so is also not safety critical. BR has used computers in these systems for thirty years.

It would appear from the quote that one of these two failed.

> An internal investigation began after an operator found

> that the system was providing "the wrong information". Realising that he had
 > lost track of train movements, the operator immediately turned all signals to
 > red.

A bit drastic ! The trains would all be following safe and valid routes.

> A spokesman said that at no time was any train at risk. "What happened caused > concern to the signalman."

True.

> The lights told him that something was different to what was happening

> [outside]." ...

> The software faults were found inside the panel in the train indicator box in

> a system responsible for operating the lights. ...

> BR conceded that the faulty equipment served a vital function ...

Vital, but not safety critical.

Paul asks:

> It would be nice to know *how* the signalman knew that he was being given
 > wrong information, and what would have happened if he had not been so alert,
 > and continued to operate the network with the wrong information.

Depending on which sub-system failed, perhaps he was seeing routes set which cross each other, or train 1E23 on his panel (this train is never less than 200km from Waterloo). Trying to operate the system blind (assuming the push-button simulator wasn't malfunctioning as well) would be awkward, but certainly less difficult than operating with all signals at red and trains moved through verbal orders.

> If, as the manufacturer states, the system is under test, why was it being run > to control live traffic without any back-up system?

First you test it on a model railway. Then you hook in the display system in parallel with the existing one, and see what happens. Eventually, however, you have to go live.

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

Ke: A Tough Roach ... [RISKS-10.17]

David Collier-Brown <davecb@nexus.yorku.ca> Fri, 3 Aug 90 11:53:16 EDT

In "Design for the Real World" (author forgotten!) televisions for hot third-world countries are discussed briefly: they're sealed, with a largish heat-sink making up part of the case.

Purchasing a computer in New York is therefor a RISK, since they don't realize they're a third-world county and take requisite steps...

--dave (:-)) c-b

David Collier-Brown, 72 Abitibi Ave., Willowdale, Ontario, CANADA. 416-223-8968



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Will Martin <wmartin@STL-06SIMA.ARMY.MIL> Thu, 9 Aug 90 12:36:58 CDT

"Run for the hills! Congress is in session!"

The following item was included in a column on printer technology in the August '90 issue of "St. Louis Computing," a tabloid freebie local paper:

"...computer printers have become so advanced that the Treasury Department is concerned that they will soon be used to print money. Michigan Senator Donald W. Riegle Jr. has introduced a bill that would make it a crime to possess any device that the Treasury Department concludes would facilitate counterfeiting." Hmmmm.... I hope the generality is in the reporting and not in the proposed legislation, because "any device" as cited above includes eyeballs, pencils, engraving tools, paper, ink, color copiers, and millions of other items both mundane and esoteric... If the legislation is actually written so broadly or vaguely, I nominate it for "dumb bill of the month".

Anyone out there know the actual details of this proposal? Will Martin

Computer voice recognition monitor for gang members

Rodney Hoffman &offman.ElSegundo@Xerox.com> 10 Aug 90 08:26:53 PDT (Friday)

According to a story by John Kendall in the 'Los Angeles Times' 10 August 1990, a computerized voice recognition system will be used in a six-month pilot program to assure that gang members on probation stay home during "Red Alerts," declared by the Probation Dept.

>From the article:

"A computer will telephone designated gang members at random during the hours they are restricted. The computer will direct them to state their names and repeat after the computer as it names several states. The computer will then electronically analyze their responses and compare the findings with voice tapes made earlier. If the computer questions any of its contacts, it will notify monitors, and a probation officer will be sent to check in person....

"Probation Department Deputy Director Michael Lindsey ... expects the computer monitor program to be in place sometime this month. If it is deemed a success, he wants to extend electronic monitoring to the entire county, with upward of 1,000 gang members in the system eventually. But first, the present program must be perfected, he says.

"The \$19,000 system employs a computer and voice-analysis software provided free to the Probation Department for six months by BI Inc., a Boulder, CO firm. Currently, four college students are preparing background information for the computer on 100 gang members. Next, deputy probation officers will record their charges' voices for comparison by computer.

"When gang trouble develops, the police and probation officers will identify the gangs involved, determine what members are on probation and tell them individually to stay home for periodic checks by the computer. Lindsey hopes that computer monitoring will afford soft-core gang members an excuse to stay out of trouble."

✓ U.S.-supplied Saudi air defense software not working

Jon Jacky <ON@GAFFER.RAD.WASHINGTON.EDU>

Fri, 10 Aug 1990 9:53:38 PDT

The following excerpts appeared near the end of a story in THE SEATTLE POST-INTELLIGENCER, Aug 10, 1990 p. A2:

BOEING FLYING FAMILIES OUT OF SAUDI ARABIA by Bill Richards

... Most of Boeing's employees work on either the Saudi's Airborne Warning and Control System (AWACS) aircraft or on the ground-based Peace Shield network. ... The \$1.2 billion Peace Shield system, which consists of a network of computerized radar and communications equipment designed especially for the Saudis, has been a problem for Boeing. The equipment was designed as a ground-based air defense system to complement the airborne AWACS, but Boeing engineers are still attempting to debug the system's softwear [sic]. The softwear is made by Computer Sciences Corp. of El Segundo, Calif. Boeing officials said Peace Shield was scheduled to be completed next year, but is behind schedule.

"The system is not up and running," Boeing spokesman Don Brannon said yesterday. Brannon said most of the Peace Shield activity underway in Saudi Arabia now involves construction work

- Jon Jacky, University of Washington, Seattle jon@gaffer.rad.washington.edu

Hubble Trouble: 'Astonishing' error of about 1 mm (excerpt)

Lauren Weinstein <CL@SAIL.Stanford.EDU> 09 Aug 90 1748 PDT

By PAUL RECER, AP Science Writer

WASHINGTON (AP) - A NASA committee investigating the focusing flaw that crippled the Hubble Space Telescope said Thursday that there was an error of about 1 millimeter in a measuring device used to grind the telescope mirrors. In the precise world of optics, such an error is ``astonishing,'' said one expert.

A one-page statement released by NASA said a committee investigating the Hubble problem found that a measuring device called a reflective null corrector had been adjusted incorrectly when the primary mirror was being ground and polished at the Hughes Danbury Optical Systems plant in Danbury, Conn. Hughes Danbury had preserved the null corrector in the exact position that had been used to grind and polish the mirrors in the early 1980s and the investigation committee tested the device on Wednesday.

Preliminary results of the test, the statement said, "have revealed a clear discrepancy of approximately one millimeter between the design of the null corrector and the device as it exists." [...]

Daniel Schulte, a senior scientist at the optical laboratory at the Lockheed Palo Alto Research Laboratory in California, said that an error of that magnitude was ``astonishing.'' ``That's gross,'' he said. ``There's no reason for an error of that size to be tolerated.'' Schulte said that in normal optical manufacturing, a tolerance of a 20th or a 50th of a millimeter is considered ``standard tolerance.'' He said the error was so large ``it had to be a transposition of numbers or something like that, that was carried through. It had to be something clerical like that." Schulte, an astronomer, was a member of an independent panel named by NASA to evaluate the Hubble focusing flaw just after it was discovered in June.

A null corrector is a device that can be adjusted to create a pattern of light in the exact shape desired in an optical lens or mirror. The light pattern from a null corrector is interpreted by another device to tell a computer the precise grinding and polishing pattern that must be followed. However, if the null corrector is set wrong, then the lens or mirror will be ground to an incorrect shape. In effect, the optics are then made to the wrong prescription and cannot give the expected focus. [...]

Ke: British Rail signalling software problem

Pete Mellor <pm@cs.city.ac.uk> Fri, 10 Aug 90 00:49:06 PDT

Many thanks to Clive Feather for explaining (<u>RISKS-10.18</u>) what probably happened when a BR signalman closed down a part of the network because he could (apparently) no longer trust the information displayed to him.

Disclaimer: I know next to nothing about railway signalling, so I could only quote the Guardian news item verbatim (but adding a few speculations of my own). Clive is obviously much better informed.

On one point, however, I do stand firm. That is the manufacturer's preposterous (at any rate, it sounded preposterous to me) claim that the system was still 'under test'.

As Clive says:

> First you test it on a model railway. Then you hook in the display system in
 > parallel with the existing one, and see what happens. Eventually, however, you
 > have to go live.

I entirely agree, but that was my point: when you go live, the system is no longer 'going through a testing stage' as the manufacturer said. If the system is 'under test', then, as Clive says, you run it *in parallel* with the existing system (as the final stage of its trial). The new system goes live, without back-up parallel systems, when the manufacturer is confident that its reliability is no worse than the system it replaces.

He can't have it both ways!

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V OHB UK

Ke: "compress" and the Unisys patent (Littman, <u>RISKS-10.18</u>)

"Anonymous" <...> Fri, 10 Aug 1990 7:58:11 PDT The message in RISKS regarding compress was unnecessarily alarming. In fact, it really represents the start of a chain of hundreds of Usenet messages discussing the Unisys patent in detail, including various postings by the compress authors. There is considerable question regarding software-only implementations of the algorithms, *which* algorithms really are involved, Unisys' true intentions, compression vs. decompression, validity or invalidity of the patent if tested in court, etc. It is not a simple situation, and there is significant evidence that some people may have become alarmed unnecessarily, or at the very least prematurely.

People who need more information about this subject should look over the entire discussion if possible, not react to the initial statement. This would seem to be a risk of seeing only the first message in a chain!

There may yet be potential complications regarding compress and the Unisys patent, but this is by *no* means an established fact at this point and is a matter of active analysis at this time.

Ke: Design for the real world (<u>RISKS-10.18</u>)

&obert.Biddle@comp.vuw.ac.nz> Fri, 10 Aug 90 14:54:32 +1200

>From our library computer: Callmark Main Collection Status : In TS171.4 P213 D 2ed TITLE Design for the real world : human ecology and social change / Victor Papanek. 2nd ed., completely rev.

NAME 1. Papanek, Victor, 1925-

IMPRINT London : Thames and Hudson, 1985. EXTENT xxi, 394 p. : ill. ;

NOTES First published: New York : Pantheon Books, 1971. Includes index. Bibliography: p. 351-385.

SUBJECT 1. Design, Industrial.

And a very interesting, if often anectodal, book it is too.

Robert Biddle, Computer Science, Victoria University, Wellington NEW ZEALAND

***** Advance notice of Computer Security Applications Conference

(Marshall D. Abrams) <abrams@soldier.mitre.org> Mon, 06 Aug 90 13:47:02 -0400

Marshall D. Abrams, The MITRE Corporation, 7525 Colshire Drive, Mail Stop Z269, Mc Lean, VA 22102 phone: (703) 883-6938 FAX: (703) 883-5639 [effective 7/10/90]

Sixth Annual Computer Security Applications Conference

December 3-7, 1990 Westward Look Hotel, Tucson, Arizona

Sponsored by American Society for Industrial Security Aerospace Computer Security Associates

in cooperation with IEEE Technical Committee on Privacy and Security American Institute of Aeronautics and Astronautics ACM Special Interest Group on Security, Audit and Control

Keynote Speaker: Senator Dennis DeConcini (D - Arizona)

Luncheon Speakers: Ralph V. Carlone, GAO Dave Fitzsimmons, Cartoonist, Arizona Daily Sun

Distinguished Lecture in Computer Security: Dorothy E. Denning, DEC

Tutorial Program, Monday, 3 December 1990

Morrie Gasser, DEC, "Security In Distributed Systems" Brett Fleish, Tulane, "Introduction to Trusted Computer System Design" Richard Linde, Unisys, "Penetration Testing" Charles Martin, Duke Univ. "Applying Formal Methods by Hand"

Tutorial Program, Tuesday, 4 December 1990

Morrie Gasser, DEC, "Security in Distributed Systems II" Teresa Lunt, SRI, "Approaches to Database Security" E. J. Humphreys, British Telecom, "OSI Security" David Snow, ITT, "Risk Management" John McHugh, CIT, "Software Safety"

Technical Program, Wednesday - Friday, 5-7 December 1990

Technical Paper Sessions

- + Trusted System Development (architecture, design, formal methods, auditing, user interface)
- + Network Security
- + Security Engineering (risk assessment, life cycle)
- + ISO Standards
- + Data Base Security (research, application)
- + Non DOD Applications
- + DOD Applications
- + Integrity

Panel Sessions

- + Computer Crime
 - + Trusted System Development
 - + Education and Ethics

- + Trusted Subject-based DBMS
- + Software Safety
- + Certification of Professionals
- + Security Standards for Open Systems
- + Computer Security in Government Labs

Special Events: Biosphere II: a prototype of the Earth for the future; Sonora Desert Museum: living animals and plants of the Sonoran Desert Region

Additional Information For a copy of the advance program, which includes rates, schedule, registration form, and special activities, contact: Diana Akers, Publicity Chair, (703) 883-5907, akers%smiley@gateway.mitre.org , Victoria Ashby, Co-Chair, (703) 883-6368, ashby%smiley@gateway.mitre.org , The MITRE Corporation, 7525 Colshire Dr., McLean, VA 22102

Advance Programs will be available early September. Please request one at that time. Conference proceedings and videotape of the Distinguished Lecture will be available. Program Subject To Change.



Search RISKS using swish-e

Report problems with the web pages to the maintainer


MYC Parking Violations Computer called "Rogue"

Dave Davis <davis@mwunix.mitre.org> Tue, 14 Aug 90 10:12:14 EDT

The 14 Aug. New York Times reports that a "Rogue Computer" is billing New Yorkers \$19 million a year for parking violations they have not committed.

City Councilman Andy Stein insists that the city must hire an independent auditor before a consulting company's contract for \$11m is renewed.

A spokesperson for the Bureau call Mr. Stein's statements "hyperbolic", adding that the bureau only makes \$4m in errors, not \$19m.

The system processes about 12m summonses a year, resulting in an average of 42,000 complaints against the city. The bureau officials feel that a resulting percentage of .003 is quite good.

Previously, the system had been operating at 82,000 errors annually.

Monday, many of those who have been unfairly ticked held a news conference.

A Mr. Hernandez, who began receiving tickets prior to being of legal driving age, has never held a license and never owened a car, (he also claims not to know how to drive) received \$4,152 in parking tickets and has had is wages attached. Another example is a individual who had his license plates stolen, reported it promptly, and still receives summonses. The bureau advises him to track down the car that bears his plates as the only solution.

In summary, we have another example of computerized bureaucracy more than a little out of control.

Computer noise linked to stress -- computers vs. women

Allan "Just say NO to postcard requests!" Meers <allans@ebay.sun.com> Mon, 13 Aug 90 21:20:17 PDT

Dr. Caroline Dow and Dr. Douglas Covert, assistant professors of communication at the University of Evansville Indiana, believe they have linked noise made by video display terminals with stress symptoms in women, who hear high-frequency sounds better than men.

The AP article, reported in the Aug 12, 1990 San Jose Mercury News (all the news we twist to fit*), reports that the couple first became interested when Dow noticed the subconciously irritating effect that a university computer she was using had on her.

Tests on 41 students in April 1987 showed that the subjects exhibited the stress symptoms of speeded up work and a doubling of their error rate when doing clerical work in a room where the high-pitched sound was created. Dow said, "We can all work through that sound, but it is tiring and distracting." They hope their research will be expanded on by others, possibly linking the noise with headaches, tension, miscarriages, and other health problems.

Men are rarely bothered by the 16 kilohertz pure-tone sound, as they generally cannot hear frequencies above 15kHz, while women can hear up to around 18 kilohertz, Dow also said. Dow and Covert were to present their findings at the Minneapolis national convention for Education in Journalism and Mass Communications.

[Also noted by Andrew E. Birner, Zenith. NOTE * I thought it was "All the news that fits we print." PGN]

Response to Computers as Counterfeiters

Sanford Sherizen <0003965782@mcimail.com> Sat, 11 Aug 90 11:54 EST

Will Martin asked about the Riegle bill that would make it a crime to possess any device that the Treasury Department concludes would facilitate counterfeiting. I don't know anything specifically about that bill but will pass on info concerning the larger issue. (Those who want the bill can contact Sen. Riegle's office or contact the U.S. Capitol switchboard ((202-224-3121)) and ask how to get a copy.)

Several years ago, the Treasury Dept. became aware that color copiers had reached a level of reproduction clarity that the technology could be used for counterfeiting. A study was done by Battelle on the issue and supposedly a recommendation was made that there be changes in U.S. currency design to prevent counterfeiting of this sort. I understand that the change was to include certain metallic-like threads that would be incorporated into the paper used for printing currency. The threads would prevent true copies from being made or, depending upon how they were used, to make it easier to spot counterfeit money since they would not look the same as the true currency when eyeballed by a bank. So far, I have not heard of the new bills being distributed or whether old currency will have to be traded in.

My guess is that the Riegle bill is not in response to that issue but more due to an article that was in Forbes Magazine last year. The article described how desktop publishing could easily be used to create false financial documents, including checks, certificates, and other documents, such as school transcripts, that could be used for financial gain. DTP fraud worries bankers, who already have come across several cases.

My guess is that the bill does not *outlaw* printers, computers, or other devices but may be an attempt to beef up the counterfeiting laws on the books and force the Treasury to determine ways to protect easily copied financial instruments. After all, Riegle is chairman of the Senate Banking Committee, where they sure know about illegal creation of funds (the Keating Five) and restricting flows of money (the Savings and Loan crisis).

Hope this stops rumors that the Feds are trying to outlaw computers.

Sandy Sherizen

Ke: 90% of research experiments fail, Risks of Statistics

Jeremy Grodberg <jgro@apldbio.com> 12 Aug 90 01:56:12 GMT

Several people have asked for references to the Scientific American article

which I mentioned in <u>RISKS 10.18</u>. The article is "Test Negative: A look at the 'evidence' justifying illicit-drug tests" by John Horgan in _Scientific American_ Vol. 262, No 3., pages 18 & 22; March 1990. The author examines the broader question of making unjustified conclusions from research findings, in the context of illicit-drug use, and concludes that on-the-job illicit-drug testing does not have any scientific justification.

Also, it was pointed out that the legend has it that Edison discovered the carbon filament, not the tungsten filament. I apologize for the error.

Jeremy Grodberg

Freedom to write programs

<rms@ai.mit.edu> Sun, 12 Aug 90 12:45:08 EDT

Programmers are now coming to grips with the fact that they are no longer free to write and distribute programs in the United States. Both user interface copyrights and software patents create monopolies on large classes of computer programs, thus restricting the programs that most of us are allowed to develop.

For example, Unisys claims a patent covers compress, which may soon be a required part of a national standard (POSIX user portability extensions). Companies delivering the supposedly free X Windows server are being threatened with lawsuits by two different companies.

The League for Programming Freedom is an organization dedicated to bringing back this freedom. The members include professors, students, entrepreneurs, and many programmers. Prominent members include Marvin Minsky, John McCarthy, Robert S. Boyer (known for fast string search), and Guy L. Steele, Jr.

The League advocates the abolition of copyright on interfaces and of software patents. It does not oppose copyright as it was understood until a few years ago--copyright on individual programs.

For more information on the patent threats mentioned above, on the League position, and on the arguments behind it, write to league@prep.ai.mit.edu and ask for the position papers.

Ke: Risks of de facto standards

<cosell@BBN.COM> Sun, 12 Aug 90 13:21:35 EDT

}Since "compress" is the de facto standard method for moving big files across
}the net cheaply ...

} They will

}either find a new data compression algorithm or send around uncompressed files
}(as soon as they can find the disk space to store the uncompressed tar files!)

Of course, sending around uncompressed files is unbelievably idiotic. That WOULD be consistent with the general FSF philosphy, which is to apparently avoid innovation at all costs and restrict their activities to implementing other people's ideas.

Plain and simple, there are zillions of compression schemes about. 'compress' is hardly the best of them, although it is quite good. Its major advantage and popularity is more accidental than that it depends on any real technical necessity [a questionably-public-domain implementation 'made the rounds', and it *IS* better than the adaptive Huffman coding compression, which is what was previously being used. And so it kind of 'snuck in'. Few people using compress have any intellectual or technical investment in it: in fact, few have any clue what the algorithm even IS: if it were changed to something else tomorrow almost no one would know or care.

/Bernie\

Kisks of inflation

Mark Brader <msb@sq.com> 12 Aug 90 14:56:22 EDT (Sun)

While on a recent visit to Scandinavia, I encountered "Ex, the magazine for Nordic airport passengers". Despite my citizenship not being Nordic :-), I read the July/August issue.

An item titled "Costly Debt" reports the sad case of Bjarne Arnhaug, of Vestfossen, Norway. It seems that he bought a lightning rod which for some reason was priced at 3040.62 kr., say about \$500 US. But Norway has eliminated its smallest coins, so that the closest you can get to making up that amount in cash is 3040.60. And when he charged the purchase, that was the amount the bank's computer billed him for.

Presumably it was the store's computer that, after 6 months, turned over the remaining debt of 0.02 kr. to a collection agency, which then billed Arnhaug for that amount plus 45.00 kr. in fees and interest!

Arnhaug's comment: "I find this a curiosity but I wonder if the debt collector has any control system when such things are allowed to happen. Computers are normally a good thing, but they must be used with common sense. ... Maybe I have a [0.02 kr.] coin hidden somewhere to give them if they are really so poor. But I am not going to pay the extra bill."

Mark Brader, SoftQuad Inc., Toronto

utzoo!sg!msb

Firing (of[f]) the Fire-Control

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 13 Aug 1990 11:41:00 PDT

I received an anonymous letter today describing a bank problem that seems

worthy of mention. However, since the anonymous contributor did not want his/her name mentioned, I shall not mention the identity of the bank either.

"At the beginning of August, 1990, the physical plant/maintenance department decided to test the fire-control system in the computer room. The part of the system that shuts off all computer power was supposed to be disconnected first. Computer operations supervision was notified first, and approved of the test. So *at the approved time* (which was *during the day*, and *in the middle of month-end processing*), the system was tested and all computer power was lost!

"The computer was down for about a day while the staff worked to restart it. [The bank] missed the deadline for the Federal Reserve's month-end requirements. All teller machines shut down, and all bank branches, too (and probably had to pay the resulting penalty/fine...).

"I'll bet they test their automatic fire control/computer shutoff system differently next time." [End of anonymous contribution]

✓ US Department Of Education --Student Loan Nightmares !!!

Steven Blair <sblair@synoptics.com> Mon, 13 Aug 90 13:23:13 -0700

Upon opening our Saturday, August 11th USmail, we were greeted by "one of those" government looking letters from the US Department Of Education. Nervously, we dropped all other USmail, and tore it open.

When we opened it, we were greeted with a intimidating letter that we owed ~\$700.00 on my wife's Guaranteed Student Loan. I remarked that I'd paid the loan off-in full in 1989 (May 31st, to be exact), and that I'd call them on Monday.

Well, I just got off of the phone with them. There's a massive problem caused by malfunctioning "new computer & new software" said the person on the other end of the phone. "let me transfer you to another extension". At that extension, a very harried man answered, I gave my story, wife's SSN, etc., and he said "your wife's account is paid in full -- you've got the "Computer Problem" also. He explained that there was a massive problem. Then, he explained that I'd be transferred to abother extension, where I could explain it to a person, who could post "Account Paid".

OK, I've now been forwarded to the next person. This person sounds worn out, like serious burnout from his job is happening. Once again I explain, give him my wife's SSN, he checks, and says "Yep, you're wife got it too"!!. I thought I'd try to find out more from this person(who had phones ringing in the background). Iasked him what the problem was, he explained "About 2 weeks ago, a new system was brought online". "The new system seems to have forgotten about 300,000 ++ paid debts". "So that machine a couple of days ago started sending out delinquent notices to all these folks". He went on to explain that the new system had been "disabled", thus rendering it unable to generate any more inaccurate bills!!!

I've got to wonder how many folks, upon seeing this notice from the govt, blindly went and paid the bill anyway thinking that they were still not paid

off on their loans.

Thank God, I got through. They're reposting that my wife's account is paid off ...

Steven C. Blair, Network Operations Center, SynOptics Communications Inc., Mountain View, California

Error blamed on human (!)

Geoff Kuenning <geoff@desint.UUCP> Tue, 14 Aug 90 01:10:36 GMT-0700

I recently received a postcard with the following text:

"Due to a human error at our computer service your renewal to VeloNews was started with the wrong issue date."

The postcard goes on to apologize and to explain how they will compensate for their error. Nice to see someone who doesn't blame the machines!

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

***** Re: Computer voice recognition monitor for gang members

<smv@apollo.com> Mon, 13 Aug 90 21:40:44 EDT

How long do you suppose it will take these probationers to forward their calls to cellular phones during "red alerts".

[Also noted by bae@auspex.UUCP (Brian Ehrmantraut) and scott@sage.uchicago.edu (Scott Deerwester)]

Virus: cautionary tale

paj <paj@gec-mrc.co.uk> 14 Aug 1990 09:38:17-BST

The following happened to a relative of mine who obtained a computer for his kids. Names have been omitted to protect the guilty:

The new computer worked, but not well: it failed to boot off one of the system disks. There followed a trip back to the store. Other computers in the store showed the same failure. The manufacturer was telephoned and abused. In desperation a virus check was run. It revealed an infection.

It transpired that before allowing a computer to leave the store, the salesman checked that the system worked and that the disks could be read. What he did



<sklein@cdp.uucp> Sun, 12 Aug 90 15:55:01 -0700

[Starkly excerpted by PGN from selections from SKlein]

There is much more to the article excerpted below, which appeared in Washington CityPaper, a weekly muckraking free newspaper distributed in and around the Washington, DC area. The article was written by Greg Kitsock, August 10th issue (Volume 10, No 32?). Washington City Paper at 724 9th Street NW, 5th floor, Washington, DC 20001. Phone (202) 628-6528. They can also be reached at MCI Mail 384-9327.

Bent Out of Shape:

Four years and millions of dollars after Challenger, NASA thinks it's got the shuttle's glitches all straightened out. But engineer Ali AbuTaha insists there are a fatal few that NASA missed.

Ali AbuTaha, an engineer with 20-years of aerospace experience traces the Challenger disaster--and future disasters if his warnings aren't heeded--to a radical change in launch procedures that was mandated by NASA officials just prior to the shuttle's maiden voyage in 1981. That change in launch procedures, says AbuTaha, has subjected every mission to liftoff forces far exceeding the hardware's safety margins.

[There is a fascinating bit about the torque while revving to full throttle before takeoff, because of the asymmetry with respect to the boosters, producing a motion known as `twang', and AbuTaha's analysis of the situation.]

"The Rogers Commission was not oblivious to shuttle "twang." But it rejected the idea that twang had anything to do with the Challenger disaster. Page 54 of the first volume of the commission's report states, 'The resultant total bending moment experienced by [the Challenger] was 291 x 10^6 inch-pounds, which is within the design's allowable limit of 347 x 10^6 inch-pounds.' However, on Page 1,351 of Volume 5 of the report, the commission cites the same figure, written as '291,000,000,' as the bending moment for the _right_ solid booster only. The effect on the entire assembly, argues AbuTaha, should be the combined bending moments of both boosters. Multiply by two, and you arrive at the maximum force that AbuTaha calculated.

"This figure is 70 percent greater than the design's allowable limit, as cited in the Rogers report. And every shuttle mission up to the Challenger explosion (and possibly afterward) has experienced this force. 'This is the kind of error that catches up with you,' warns AbuTaha.

"Not only does this miscalculation explain the shuttle disaster that killed seven astronauts and set our space program back nearly three years, as AbuTaha suggests, it also reveals the source of the mysterious malfunctions that have plagued the shuttle program since its first launch in 1981, from tiles knocked off and booster segments warped to satellites that inexplicably failed to work."

RISKS of preventive maintenance

<pjyp%zaphod@gargoyle.uchicago.edu> Tue, 14 Aug 90 16:19:49 CDT

I was amused by the article about the store which inadvertently virussed the disks of every computer it sold in "checking" them to make sure they wold work. I have the following similar story:

At Harvard, there is a large room full of computers (mostly macintosh) in the basement of the Science Center for students to use to write papers, etc.

Because a lot of software is available "for loan" from a software library in an adjoining room, this setup is obviously very vulnerable to viruses.

It seems that "those in the know," in order to combat this problem, have set up one computer running some disinfectant-type program or other constantly; it is the "disinfecting station" and there are signs posted to tell students and other users to make sure to disinfect all their disks on a regular basis.

The RISK is clear: although their anti-virus program is very effective, sooner or later, a virus will be invented which will elude its defenses. And then all these students will be swapping their disks in and out to make sure they won't get any viruses ...

== pj karafiol

✓ Computer-personalized scams

Allan "Just say NO to postcard requests!" Meers <allans@ebay.sun.com> Tue, 14 Aug 90 14:58:25 PDT

A couple people here at Sun have gotten phones calls from "MST" in Kansas City, offering free magazines "because of our good subscription records". Mine came to my office phone, while others have gotten them at home.

They will give you 4 magazines free, for 60 months at no charge. "No charge? Absolutely free???" says us.

"Well, there's a minor processing fee of \$2.30 a week."

Which comes out to \$120.00 per year for 4 magazines. click

After hearing from others how the magazines were pretty much tailored to their interests (computers, sports, whatever), it seems that they probably are simply using a computerized mailing list to generate calls to subscribers about other publications in the same category as their hobbies and interests. Nothing special about that - their only hope is that people fall for the \$2.30 a week ploy.

Well, you could generate a fairly accurate list of interests from Usenet, if you could compile stats of what newsgroups people read regularly. Scanning someone's .newsrc file (or whatever is appropriate for their reader), could be done under program control (sort of a Nielson service), looking for groups in which the user has marked articles to be read or whatever. The news lists "arbitron" program does something like this, but does so anonymously and with no commercial intent.

Rumors periodically circulate that someones manager is suspected of snooping by checking out what newsgroups his charges are reading this way.

So what kind of magazine offer will I get if I read alt.flame?

Compress patent

Richard Stallman <rms@ai.mit.edu> Wed, 15 Aug 90 18:02:22 -0400

Someone recently expressed the opinion that the uncertainty over the validity of the compress patent means there is no reason to be alarmed today.

I think this conclusion is inadvisable. The validity of any patent is uncertain until there is a lawsuit. That does not mean it is wise to ignore this problem until a suit is decided.

The problem with compress is a little like that of global warming: by the time you can be sure the problem is real, it is too late to solve it easily. The more the use of compress spreads, the harder it will be to stop using it, if and when Unisys threatens to sue you. The prudent thing to do is to stop now when it is easier to do.

This patent is important for another reason as well: it shows us the kind of trouble patents are likely to cause. If you are lucky this time, and either Unisys never sues you or they lose a suit, that doesn't mean you will be lucky with the next patent. Thus, the compress patent should serve as a warning about the danger of software patents.

If you would like to challenge Unisys in court and try to defeat the patent, by all means do so. But this can solve only a small part of the problem of patents. Fighting one patent at a time is prohibitively expensive and you can't expect to win each time. The only way to solve the whole problem is to make software exempt from patents.

Re: Risks of de facto standards

<davidsen@crdos1.crd.ge.com> Wed, 15 Aug 90 13:01:51 EDT

If the algorithm on compress were changed tomorrow, every person who ever used the old one would be unable to recover the data from the compressed form. I think that's a far cry from "almost no one would know or care."

More improtant, the performance of compress (bytes/cpu-sec) is very good compared to the other available programs. I ran a test on this (for other reasons), and found that compress is a factor of four faster (CPU) than any of the other compressors. It is not by any stretch the best in terms of compression, but an increase that large in time to compress news batches would make news impractical on many machines.

Here's a subset of the test results, for a typical news batch (text). Times are in sec, measured by the kernel, on a 25MHz 386 running V.3.2. Note that the size for the archivers includes a directory.

CPU final COMMENTS Program sec size (original 56718 bytes)

0.78 25486 compress 1.96 28178 archiver 200 2.84 29284 archiver (w/ "squash") arc zip v1.02 21031 archiver, run under MSDOS 3.76 lharc v2 (beta) 6.93 20602 archiver, run under MSDOS 22952 archiver lharc v1 7.12 lzhuf 7.64 22918

Hope that sheds some light on the discussion. There does not seem to be anything as fast currently available (to me).

bill davidsen (davidsen@crdos1.crd.GE.COM -or- uunet!crdgw1!crdos1!davidsen)

Ke: Risks of de facto standards

SILL D E <de5@stc06.ctd.ornl.gov> Wed, 15 Aug 90 09:24:15 EDT

In fact, the FSF's raison d'etre is to encourage innovation by making it unnecessary for programmers to write code that's already been written. The GNU project is in a drudgery phase right now since they *are* having to rewrite much existing code. At least these programs are being improved as they're being rewritten. GNU Tar, for example, does incremental backups. Their most successful product, GNU Emacs, was the original idea of the FSF's founder, Richard Stallman.

>Few people using

>compress have any intellectual or technical investment in it: in fact, few have >any clue what the algorithm even IS: if it were changed to something else >tomorrow almost no one would know or care.

Not true. Although the LZW compression algorithm is transparent to users of compress, as it should be, files compressed using it couldn't be uncompressed by a replacement program. The existing base of compressed files in public archives and private systems combined with the nearly ubiquitous presence of compress, uncompress, and zcat on today's UNIX systems would make a switch to an alternative method far from easy, fast, or transparent.

Dave Sill (de5@ornl.gov) These are my opinions. Martin Marietta Energy Systems, Workstation Support

[Also commented upon Jay Plett <jay@silence.princeton.nj.us>]

Re: Freedom to write programs

<henry@zoo.toronto.edu> Wed, 15 Aug 90 12:39:52 EDT

>For example, Unisys claims a patent covers compress, which may soon be a

>required part of a national standard (POSIX user portability extensions).

As an aside, it should be noted that inclusion of patented technology in national standards is nothing new, when it is considered the best approach and when the patent holder is willing to promise reasonable licensing. (The inclusion of compress in POSIX is, last I heard, conditional on such a promise from Unisys.)

A good example of this is Ethernet, overwhelmingly the standard mediumperformance LAN, which is a national standard despite being covered by Xerox patents. Almost nobody realizes that Ethernet is patented and that your Ethernet equipment supplier is paying royalties to Xerox. This is a good example of managing patents properly: the inventors profit and the public interest is nevertheless well served. Unfortunately, it's not always that way.

Henry Spencer at U of Toronto Zoology utzoo!henry

// credit "doctors"

King Ables <ables@mcc.com> Wed, 15 Aug 1990 14:40:17 CDT

In the Wall Street Journal of Tuesday, August 14, 1990, on the front page, there is a VERY interesting story about so-called credit doctors. People who will, for a fee, help you fix your credit rating.

Some people who provide this function are legitimate. Some are not. There are several methods detailed in the story that are used (illegally) to allow people with bad credit to obtain more credit.

One of the more frightening examples was where a customer with bad credit enters such a place and for a fee, is provided with information to be used to apply for credit. Among this new information is a "newly assigned" social security number (the client claimed ignorance of illegal doing, but getting a ssn from anyone OTHER than the Social Security Administration, not to mention getting a NEW one at all, seems like it should be a BIG red flag!). The "credit doctor" has used bought or stolen access codes on credit bureau computers to search (note, this is a READ-ONLY operation) the database for other people with identical or similar names. He then copies down THAT PERSON'S ssn, address, mother's maiden name, whatever is there and provides it to his client with instructions that it be used when making new credit applications.

Of course, eventually, when the client (either intentionally or because of continued bad financial habits) defaults on a payment, the credit bureau comes after the poor slob whose information was lifted. One woman is STILL trying to get things sorted out and people won't extend her credit now even though her file lists her as a victim of fraud.

People named John Smith should be quaking in their boots. :-(

The credit bureaus are claiming this particular hole is plugged now by

requiring more information about someone before being able to call up their credit record.

Another method was to (legitimately) contest all bad references in a client's file. By law, all contested references cannot be reported for 90 days until things are cleared up. During that 90 days, the client can apply for all kinds of credit and have a favorable credit report. This is clearly an abuse of the system that should be fixed within the system. The victim here is the merchant who unknowingly extends credit to someone who doesn't deserve it, who may or may not receive payments due at some time in the future.

All around a pretty scary article. Obviously not enough thought has gone into our system of maintaining credit information. One of the "credit doctors" claimed to be forcing a change to a broken system (and therefore justifying his actions for the common good!). The implication is that the whole credit system may be changing (mutating?) very soon.

King Ables	Micro Electronics and Computer Technology Corp.
ables@mcc.com	3500 W. Balcones Center Drive
+1 512 338 3749	Austin, TX 78759

[This came up almost two years ago, in a note by Donn Seeley, <u>RISKS-7.50</u>, 12 September 1988, citing an article "Clean Credit for Sale: A growing illegal racket", by Larry Reibstein with Lisa Drew, Newsweek 9/12/88, p.49. But for our newer readers, this revisit is worth including in RISKS. PGN]

Computerized monitoring of "house arrest" detainees

Will Martin <wmartin@STL-06SIMA.ARMY.MIL> Wed, 15 Aug 90 14:57:59 CDT

The posting in <u>RISKS-10.20</u> on gang members subject to computer voice recognition while under detention and avoiding it by forwarding their calls to cell phones reminded me of this:

Over the past weekend, here in the St. Louis area, there were a string of gas station robberies. A man who was under one of those "house arrest" restrictions, with an electronic device fastened to his ankle and a sensor in his home, linked to the telephone, was arrested and charged with these crimes. It turned out that, while the computer (a PC) that monitors these detainees works 24 hours a day, 7 days a week, the humans who have the duty of checking the computer's output work a 9-to-5 5-day-week schedule, so nobody was there over the weekend to notice that the computer had been reporting that this guy was not at home. This was in a particular Illinois jurisdiction, I believe. (I don't think they have this program operating in St. Louis City yet.)

Of course, the publicity about this now has notified all such detainees that they are 'free' over the weekends. Of course, their 'escape' will be discovered Monday morning, and they then could be jailed (if caught) for breaking the terms of their detention.

Anyway, after seeing that RISK item about call-forwarding, I immediately

thought of the following: These detainees could all get together for a party and still remain undetected if they conspired together to all meet at the residence of one of the group. Each of the others would set their own phones to call-forward to that site. That call-receiving phone would have the electronic sensor attached, and, thus, when a call was placed to any of the detainees' phones, it would be answered at the meeting site, and the sensor on that phone would properly report that the detainee wearing the device that responds to the code sent was in fact there. [They would be vulnerable only during the travel time it takes to get from their residences to the meeting site, and could probably arrange to travel during the interval between calls.]

Would this deception be detectable by the monitor? Are the sensors and ankle-units made as a pair, so the sensor will only interact with its own particular ankle unit? Or are the sensors generic, so they will just detect if the ankle unit asked about is in range? For that matter, are the ankle units coded to the individual detainee, so that the system queries if unit "1232" is in range, or does the system just check to see if any ankle unit is in range?

If the sensors are generic, then the next step after the meeting for the party would be for a confederate of one of the detainees to go to his residence, and remove the sensor unit from the phone. (Remember the detainee is already away at the other site, and being detected by the sensor there. So no one should detect this removal.) Then that sensor is attached to a cellular phone, which is given to the group of detainees. They then set the meetingplace-site phone to call-forward all calls to the cellular phone, and provide power for that sensor unit attached thereto. Thus they can then travel about as a group and engage in a crime spree, with a perfect alibi -- the computerized records will still show them all at their respective homes under electronic detention!

This won't work if the sensor only detects its matching ankle unit, but I would guess that having the sensor just be a device that would get an ankle-unit code from the computer and query the neighborhood for that code's presence would be cheaper and simpler, avoiding problems like having to reprogram a sensor when an ankle unit is broken, and thus would be more likely for budget-limited municipalities.

It also won't work if I have the wrong idea about how these things operate. I'm assuming the monitor site calls the sensor-equipped phones, and they don't do anything like detect when the ankle unit leaves their range and call in and report that fact.

I donate this idea to the public domain; if you write a "movie of the week" screenplay based on it and become rich and famous, you can put my name in the credits as "Original idea by ...". :-)

Will Martin

Ke: Computer voice recognition monitor for gang members

Paul Shields <shields@nexus.yorku.ca> Thu, 16 Aug 1990 10:50:29 -0400 I hope the system uses a challenge/response strategy of some kind, because otherwise it could be defeated by recording a voice and playing it back at the appropriate points.

Paul Shields

✓ Edison and workplace drugs (Re: Grodberg, <u>RISKS-10.20</u>)

Gordon LETWIN <gordonl@microsoft.UUCP> Thu Aug 16 10:21:01 1990

An amusing juxtaposition of topics, since Edison was very fond of a wine drink which contained considerable amounts of cocaine. According to contemporary reports, it consumed it in considerable quantities. Remember back in school when you were indoctrinated with the "Thomas Edison" story - about how he'd work all night and only get a few hours of sleep a day - now you know why.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Christopher Jewell <chrisj@netcom.UUCP> Wed, 15 Aug 90 16:09:21 PDT

1. I'm glad that the New York Times headline put quotes around `Rogue Computer': it's surely a matter of lousy software design or persistent operational errors, rather than some real-life HAL from the movie _2001_, and the Times seems to know that. (I _hope_ that the readers caught the implication.)

2. The Times quotes PVB spokescritter Stephanie Pinto, as saying that if you divide 42,000 (errors) by 12 million (tickets) you get 0.003, (0.0035 actually) and asking ``Is three-tenths of one percent reckless?''. If my bank posted 3

out of every thousand transactions to the wrong account, I'd certainly take my money elsewhere. You'd better believe that the bank's CEO would transfer the operations VP to the mailroom in short order, too.

3. Stein's rhetoric (``... rogue computer ... terrorizing ...'') is overblown headline-grabbing, but the problem is real, and both bringing in an outside auditor and installing safeguards sound like good, albeit sadly overdue, ideas.

American Management Systems of Arlington, VA was hired in 1984 to design the new system. A document written by the bureau's computer managers in 1985 outlined ``critical structural deficiencies'' and warned of ``profound and far-reaching implications.''

4. The contractor was not competent to do the job. They have delivered trash in return for their \$11 million so far. (That is for developing the software *and* running the system for the PVB.) Would a grep of the RISKS archives find other stories about lousy work by American Management Systems? That name rings a bell. [No bell prizes that I could find since Vol 7. PGN]

5. If PVB management permitted the contractor to implement the design after their own computer folks pointed out serious deficiencies, it's hard to avoid a choice between the hypotheses of stupidity and bribery. If, on the other hand, the contractor was required to correct the errors in the design, then the same choice of hypotheses applies to those responsible for monitoring contract compliance.

6. Once the system had been implemented, it is possible that management decided to install the system, not due to either stupidity or corruption, but rather on the basis that 42,000 errors/year is better than 85,000.

Note that #6 does not contradict #5: the ``lesser evil" hypothesis may apply to the decision to install the new piece of @#\$%, but it cannot excuse a decision to permit the contractor to implement a known bad design in the first place.

7. Speaking now as a former New Yorker, the PVB has been one of the more obvious centers of corruption in that corrupt city gov't for decades. This is not `whisper behind the hand' stuff: during the Koch administration, a county leader of the Democratic Party committed suicide when his part in PVB corruption came to light in an investigation that was making headlines even without the suicide. If #5 turns out to be a matter of corruption, rather than mere stupidity, few New Yorkers will be surprised.

On the other hand, stupidity about computing is *also* a tradition in the NYC gov't: the NYC Human Resources Administration used to pay tens of thousands of employees with a payroll system written in OS/360 Fortran, using type REAL*8 for money, and wonder why the pennies never seemed to balance. :-((No, they were not smart enough to avoid fractional parts by storing amounts in pennies rather than dollars.)

Chris (Christopher T. Jewell) chrisj@netcom.uucp apple!netcom!chrisj

✓ Debt collector proposes "total knowlege" credit database

Ret.) Tue, 21 Aug 90 11:56:59 EST

>From the Sydney [Australia] Morning Herald, August 20th, 1990

"Sorry, you can't afford it"

CANBERRA: Debt collectors believe that in the not too distant future there will be "total knowledge" about all individuals and envisage the Government allowing financiers to build enormous data banks which would include confidential tax file number information. In fact, they believe banks and other lenders will have so much information that debt collectors will be made redundant.

The Orwellian vision is contained in an article "Back to the Future for Commercial Agents", published in the Institute of Mercantile Agents' journal, The Mercantile Agent. Its author, Mr Norman Owens, a former president of the institute and owner of a debt-collecting agency, told the Herald that governments would one day see it as "desirable" to link together and make public all the enormous data bases containing highly sensitive personal information.

"Tomorrow's credit grantor will be extending credit in a perfect market with total knowledge of the debtor," Mr Owens asserted. "The credit grantor in the future will have access to all the debtor information. This will be made available through linked data bases in the manner of George Orwell's 1984. "

Credit cards will be of the "smart card" variety which will be "genetically engineered implants" that capture all transactions from cradle to grave. (In fact, Westpac [a major Australian bank] is working on a smart card which has a small computer chip that records all transactions and makes credit cards more secure.)

Credit files, like those held by the Credit Reference Association, will be linked to the Government's tax file number data base. "Some time in the future," he told the Herald, "mercantile agents won't exist. This is because there would be total knowledge about every individual including assets, income, credit history, and any future liabilities. The debt collector exists to catch those debtors that escape the creditor's receivable system. For most part the holes in that system will disappear in a business society armed with perfect knowledge about all transactions," he said.

Mr Owens conceded that this may sound like science fiction, but insisted that it was "science possible". He acknowledged that the community was horrified by such Orwellian plans and said the Government was adamantly opposed to it, but he was confident that one day people and governments would realise that such measures were of benefit to society.

[The thing I personally found most frightening about Norman Owens' comments - aside from the total lack of concern about possible risks - was his choice of words. Words like "perfect market", "total knowlege", "genetically engineered implants", and - of course - "benefit to society". I also must add that the

basis for his Orwellian vision is the inclusion of tax file number information currently retained by the federal government. Under current laws, this information is confidential, so his proposed scheme would be illegal. -- PH]

More on Computerized Monitoring of "House Arrest" Detainees

Li Gong <li@diomedes.UUCP> Thu, 16 Aug 90 17:22:38 EDT

Monitoring "house arrest" detainees is equivalent to a common issue in computer security. It is known as user authentication -- determinating that a particular person is at a particular location at a particular time.

Reading the research literature on the subject of user authentication shows that the current solutions depend on co-operation of a typical user. For example, he won't reveal passwords to others, and won't comprise physical security in case he uses auxiliary devices such as smart cards or credit cards. And maybe more important, he stands to lose something if someone else can successfully masquerade as him.

In the case of detainees, none of these assumptions holds. Plus the easy and wide availability of such devices as master remote control unit, which can learn signals generated by other devices of a similar type, it seems that no cheap (and thus practical) solution is in sight, unless one can assume that no one would attempt to grasp the potential forgery market.

Li GONG, Odyssey Research Associates, Inc.

Mailand computer system

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Fri, 17 Aug 90 10:18:23 EDT

(From July 1990 Privacy Journal, Vol. XVI, No 9, Page 1)

TRUE COLORS

Thailand -- a constitutional monarchy with a parliament largely dominated by the military -- has taken the Orwellian step that most Western democracies have been afraid to take. The Thai government this month inaugurated a centralized database system to track and to cross-reference vital information on each of its 55 million citizens.

The system includes a Population Identification Number (PIN) with a required computer-readable ID card with photo, thumbprint, and imbedded personal data. The system will store date of birth, ancestral history, and family make-up and was designed to track voting patterns, domestic and foreign travel, and social welfare. Eventually 12,000 users, including law enforcement, will have access by network terminals. It is the largest governmental relational database system in the world. In the private sector, only the Church of Jesus Christ of Later-Day Saints, the Mormon Church, has a larger one. "The people feel that

the system will protect them," says the director of the Central Population Database Center in Bangkok.

What is more curious than the ambitious system itself is the fact that the federally-sponsored Smithsonian Institute chose -- on behalf of all Americans -- to honor the Thais for their efforts. The second annual Computerworld Smithsonian Award for innovative information technology in the governmental sector went last month to the Thailand Ministry of Interior for its oppressive system for keeping tabs on its citizens. Something to ponder: Two of the three judges making the award have major computer responsibility in the U.S. government.

[The Privacy Journal, an independent monthly on privacy in a computer age, is a wonderful source for this stuff. Individual subscriptions are \$35/year; Privacy Journal, P.O. Box 28577, Providence RI, 02908.]

A backup that worked

<smb@ulysses.att.com> Fri, 17 Aug 90 09:34:50 EDT

Amidst all our stories of systems that have screwed up, it's worth noting one that did work as planned. The New York Federal Reserve bank's Fedwire EFT system was in the area blacked out by the New York power outage. Its backup diesel generators kept things running for several days. When one showed signs of faltering, they moved operations to a backup site outside of the city. That backup site had been established 3 years ago for exactly such contingencies.

--Steve Bellovin

NCSC to be shut down

<davy@itstd.sri.com> Sun, 19 Aug 90 12:13:42 -0700

By John Markoff, New York Times Reprinted in the San Jose Mercury News, 8/19/90 [Starkly excerpted by PGN.]

COMPUTER SECURITY CAMPAIGN SHUT DOWN Reagan-era drive targeted espionage

President Bush has ordered a quiet dismantling of an agressive effort to restrict sources of computerized information, including data bases, collections of commercial satellite photographs and information compiled by university researchers. [...]

Agency being disbanded

This month the security agency began disbanding its National Computer Security Center, moving most of its 300 employees into new jobs in the more secret communications security section inside the agency. [...]

[Most of the functions of NCSC are intended to remain, however. PGN]

Mow to Lie with Statistics [once again]

"N H. Cole" &ole@qgb.bristol.ac.uk> Mon, 20 Aug 90 13:28:24 BST

With regard to the unreliability of statistics, the only solution is to make Darrell Huff's book "How to lie with statistics" a compulsory text at all schools. It is, I believe, the source of the quote "97.43% of all statistics are made up."

Nigel Cole

Something good about Automatic Bank Tellers

Pete Mellor <pm@cs.city.ac.uk> Tue, 21 Aug 90 11:03:20 PDT

Despite the danger of severe shock to RISKS readers who see this, I thought that someone should give due credit to the designers of a particular ABT which is run by the National Westminster Bank, and an example of which is installed at City University.

Last week I drew some money on my way to lunch. As usual, I requested a receipt. When my service card popped out, I put it back in my wallet, but (being a bit more preoccupied than usual) walked away without collecting the money or the receipt. I realised my mistake one minute later when I reached into my pocket to pay for a beer, and sprinted back to the machine, only to find the receipt dangling out of the slot, but no cash. I had no option but to draw some more money and make the best of it.

I was puzzled that there had been nobody around at the time who would have been likely to have seen my mistake, and made off with the cash, so I rang the bank. They explained that this type of till, in which the money comes out through rollers, gobbles the money back if it is not pulled out of the rollers within ten seconds. Sure enough, when they 'agreed' the till the next day, they found it in credit by the amount I had forgotten, and a record of a 'customer time-out'. So they promptly credited my account with that amount.

Now, *that's* what I call user-friendly! :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V OHB

13th National Computer Security Conference, October 1-4, 1990

Jack Holleran &olleran@DOCKMASTER.NCSC.MIL> Thu, 16 Aug 90 23:58 EDT

[Jack sent me the entire registration packet for the conference on-line. It is much longer than just about any previous RISKS issue, so I have highlighted the program here. This is generally the definitive get-together for security developers and practitioners. For those of you wishing the packet, please send him mail or FTP it from CRVAX.SRI.COM in the usual directory as RISKS-10.NCS90 . Registrations before 1 Sept 90 save \$25; otherwise \$250. PGN]

Omni Shoreham Hotel, 2500 Calvert Street, NW, Washington, DC 20008 (100 yards from Woodley Park Metro Station)

SPECIAL EVENTS: October 2, 1990

Opening Plenary Session

0900 Welcoming RemarksKeynote Address, Robert G. Torricelli, U.S. Representative (D - NJ)1830 Conference Reception

Smithsonian American History Museum

October 3, 1990

1800 Conference Banquet (Omni Shoreham Regency Ballroom)
 Speaker: Ms. Michelle K. VanCleave
 Assistant Director for National Security Affairs
 Office of Science and Technology Policy
 Executive Office of the President

October 4, 1990

1100 Closing Plenary Session

Panel: Towards Harmonized International Security Criteria

1225 Closing Remarks

TRACK A - Research & Development

MONDAY, OCTOBER 1

1600 Panel: Commercial Development & Evaluation of Trusted Systems: An Open Discussion -- Our Success to Date

TUESDAY, OCTOBER 2

Verification

1030 PAPERS Covert Storage Channel Analysis: A Worked Example Verification of the C/30 Microcode Using the State Delta Verification System UNIX System V with B2 Security

1400 PANEL: Access Control: Time for A Retrospective

Electronic Authentication & Biometrics 1600 PAPERS Key Management Systems Combining X9.17 and Public Key Techniques Electronic Document Authorization The Place of Biometrics in a User Authentication Taxonomy Non-Forgeable Personal Identification System Using Cryptography and **Biometrics** WEDNESDAY, OCTOBER 3 Intelligent Tools I: Auditing **0900 PAPERS** An Audit Trail Reduction Paradigm Based on Trusted Processes The Computerwatch Data Reduction Tool Analysis of Audit and Protocol Data Using Methods from AI Intelligent Tools II: Intrusion Detection **1100 PAPERS** A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks A Neural Network Approach Towards Intrusion Detection PANEL: Data Categorization and Labeling 1600 Panel: R&D Activities THURSDAY, OCTOBER 4 Modeling **0900 PAPERS** A Generalized Framework for Access Control: An Informal Description Automated Extensibility in THETA **Controlling Security Overrides** Lattices, Policies, and Implementations **TRACK B - Systems** MONDAY, OCTOBER 1 0900 PAPER NIST/NSA Services & Publications 1400 PANEL: Computer Security Standards **Embedded Systems** 1600 PAPERS The Role of "System Build" in Trusted Embedded Systems Combining Security, Embedded Systems and Ada Puts the Emphasis on the RTE **TUESDAY, OCTOBER 2** 1030 PANEL: Disclosure Protection of Sensitive Information Network Security I 1400 PAPERS Considerations for VSLAN(TM) Integrators and DAAs

Introduction to the Gemini Trusted Network Processor An Overview of the USAFE Guard System

Network Security II 1600 PAPERS Mutual Suspicion for Network Security A Security Policy for Trusted Client-Server Distributed Networks Network Security and the Graphical Representation Model

WEDNESDAY, OCTOBER 3

System Test & Integration 0900 PAPERS Testing a Secure Operating System An Assertion-Mapping Approach to Software Test Design Security Testing: The Albatross of Secure System Integration?

Network Standards

1100 PAPERS

Low Cost Outboard Cryptographic Support for SILS and SP4 Layer 2 Security Services for Local Area Networks

Operating Systems 1400 PAPERS Trusted MINIX: A Worked Example Security for Real-Time Systems Trusted XENIX(TM) Interpretation: Phase I 1600 PANEL: Vendors' Activities

THURSDAY, OCTOBER 4

Viruses 0900 PAPERS PACL's: An Access Control List Approach to Anti-Viral Security Static Analysis Virus Detection Tools for UNIX Systems The Virus Intervention and Control Experiment Classification of Computer Anomalies

TRACK C-I - Management & Administration

MONDAY, OCTOBER 1

Contingency Planning & Disaster Recovery (Part I) 0900 PAPER Disaster Recovery / Contingency Planning 1100 PANEL: Professional Development

Contingency Planning & Disaster Recovery (Part II) 1400 PAPER Disaster Recovery from \$138 Million Fire 1600 PANEL: Plans and Assistance

TUESDAY, OCTOBER 2

Criteria: National & International **1030 PAPERS** Harmonised Criteria for the Security Evaluation of IT Systems and Products The VME High Security Option Rainbows and Arrows: How the Security Criteria Address Computer Misuse Civil and Military Application of Trusted Systems Criteria 1400 PANEL: Implementation of the Computer Security Act of 1987 Approaches to Trust **1600 PAPERS** The CSO's Role in Computer Security Implementation and Usage of Mandatory Access Controls in an Operational Environment Building Trust into a Multilevel File System WEDNESDAY, OCTOBER 3 **Risk Management** 0900 PANEL: Risk Management **1000 PAPERS** LAVA/CIS Version 2.0: A Software System for Vulnerability and Risk Assessment WORKFLOW: A Methodology for Performing a Qualitative Risk Assessment Critical Risk Certification Methodology Acquisition 1400 PAPERS Factors Effecting the Availability of Security Measures in Data Processing Components Integrating Computer Security and Software Safety in the Life Cycle of Air Force Systems 1500 PANEL: Acquisition Discussion Integrity 1600 PAPERS Integrity Mechanisms in Database Management Systems A Taxonomy of Integrity Models, Implementations and Mechanisms THURSDAY, OCTOBER 4 0900 PANEL: National Computer Security Policy TRACK C-II - Management & Administration MONDAY, OCTOBER 1 DATABASE MANAGEMENT 0900 TUTORIAL: Database Management Systems and Secure Database Management Systems 1100 PANEL: A Year of Progress in Trusted Database Systems 1400 PANEL: Trusted Database Systems: The Tough Issues 1600 PANEL: Multilevel Object Oriented Database Systems

TUESDAY, OCTOBER 2 C2 Microcomputer Security **1030 PAPERS** C2 Security and Microcomputers Functional Implementation of C2 by 92 for Microcomputers 1400 PANEL: Electronic Certification: Has Its Time Come? 1600 PANEL: Defense Message System (DMS) Security WEDNESDAY, OCTOBER 3 0900 PANEL: IEEE Computer Society Limited Access to Knowledge and Information 1100 PANEL: Computer Emergency Response Team: Lessons Learned Ethics 1400 PAPERS Discerning an Ethos for the INFOSEC Community: What Ought We Do? VIRUS ETHICS: Concerns and Resonsibilities of Individuals and Institutions Concerning Hackers Who Break into Computer Systems 1600 PANEL: National Institute of Standards and Technology Activities THURSDAY, OCTOBER 4 0900 PANEL: Hackers: "Who are They?" Track D - The Computer Security Tutorial Track MONDAY, October 1 **0900 PAPERS** Automated Information Security: Overview of the Tutorial Security Overview and Threat Information Security Life Cycle Management Requirements **Risk Management** TUESDAY, October 2, 1990 **1030 PAPERS** Data Security Physical, Personnel and Administrative Security Office Automation Security WEDNESDAY, October 3, 1990 0900 PAPERS **Telecommunications Security** Software Controls **Trusted Systems Concepts**

Trusted Network Concepts





<kjd@rust.zso.dec.com> Wed, 22 Aug 90 11:37:09 PDT

PORTLAND, Ore. (UPI) -- Hundreds of automated bank teller machines on The Exchange network in Oregon and Washington went on the fritz this week, a problem officials traced to a computer software glitch.

The network includes most major financial institutions in Oregon, except for First Interstate Bank.

Tom Bass, president of The Exchange, based in Bellevue, Wash., said the problem was ``a certain segment of the computer overloaded, and it had to be rebalanced."

One Portland woman said she put her card in a machine to withdraw some money and got a slip back showing the withdrawal but no cash.

In other cases, customers using about 400 machines put in their cards,

watched the machine process their transactions and got their card back, but no receipt. Others got no money, only a receipt showing that their request to withdraw cash had been denied.

Bass said Tuesday the problems had been corrected but that officials were watching closely to prevent any repeat. He said the system can detect errors and correct them automatically but advised anyone who has difficulties with the machines to contact their bank's customer service department.

Formal Verification of Safety-Critical Systems

Brian Randell &rian.Randell@newcastle.ac.uk> Mon, 20 Aug 90 16:46:04 BST

As I know from personal experience, recommending an article on formal verification to the RISKS readership is itself a risky act. Nevertheless let me, with some trepidation, recommend (without necessarily agreeing totally with) the paper "Formal Verification of Safety-Critical Systems", by Moser and Melliar-Smith, that has just appeared in the August 1990 issue of Software Practice and Experience.

The paper's abstract is as follows:

"We describe our practical experience in the use of formal verification to obtain increased confidence in the design of safety-critical systems. The experiment involved demonstrating the consistency of the design specifications of SIFT, a software-implemented fault-tolerant operating system for aircraft flight control. Specifications were written at successive levels of abstraction from the most abstract requirements definition down to the detailed level of program code. Consistency of the successive levels of specification is demonstrated using the enhanced HDM verification system. Formal verification is currently feasible only for carefully simplified systems, but there appears to be no alternative method that can meet the extreme safety requirements for safety-critical systems."

Apart from the description of the SIFT experiment, I regard the article as notable for its discussion of the advantages and disadvantages of software testing, software fault tolerance, safety kernels, fault tree analysis, and (in much more detail) formal verification.

Quoting from the paper's section entitled "Can Verification Ensure Safety?":

"Formal verification is an elusive approach to achieving safety in computer systems. It is clear that whatever is demonstrated by formal verification is demonstrated with almost absolute certainty. But what is it that is demonstrated by formal verification and is it what is needed for safe operation?

Strictly speaking, formal verification only demonstrates a mathematical relationship between a mathematical representation of the requirements or specification of the system and a mathematical representation of the design or program code. Before we can assert that the verification has any significance, we must be confident that

- 1. The top-level specifications or requirements are correct and sufficient to ensure the properties we need a major problem.
- 2. The mathematical representation of the specifications means what we think it means and the verification system does not permit invalid proofs usually not a problem.
- 3. The mathematical representation of the program code is identical to the actual code often it is not.
- 4. The formal semantics of the programming language and the verification conditions constructed for the program accurately reflect our intent for the language a problem only for difficult constructs such as concurrency.
- 5. The implementation of the design or program code, including compilation and instruction execution by the underlying computer, is correct another significant problem.
- 6. The fault models are realistic models of the risks of faults in the system."

Some of the authors' overall conclusions will, no doubt, arouse controversy, but nevertheless are I think worth quoting from here:

"Within the current technology, formal verification is a possible approach for small sets of safety properties in clean simple carefully-designed systems, where the cost of failure is high enough to justify the cost of verification. Examples of such systems include nuclear reactor safety shutdown systems, simple security systems such as red/black encryption schemes, and simple operating system kernels. To be verifiable such systems must be highly restricted in their levels of complexity, and desired features may have to be sacrificed.

It is clear that it is still infeasible to verify typical real systems of sizes in the tens and hundreds of thousands of lines of code. Examples of systems that are still infeasible are nuclear control systems, aircraft flight control systems, and multi-user secure operating systems.

For systems that must be very safe, there appears to be no alternative to verification. Testing, fault tolerance, and fault tree analysis can make important contributions to safety, but they alone are unlikely to achieve the high levels of safety that are necessary for safety-critical applications. Without improved verification systems these applications should not be certified at the level of 10**-10 safety-critical failures per hour.

Formal verification is, therefore a critical enabling technology for many important applications, both civil and military. It is far from clear that imminent advances in verification technology will suffice to render feasible the verification of these systems. A realistic time-scale for the improvement in verification technology required to verify real systems cannot be less that twenty years, even assuming sufficient interest and funds.

Unfortunately, interest in and support for research in formal verification has been limited and, consequently, progress has been slow. Potential users have been reluctant to accept verification for fear that they may be forced into premature use of a technology that is currently difficult and costly to apply. This reluctance is bolstered by wishful thinking about techniques, such as software fault tolerance, that are easier to apply but that are unlikely to achieve the high levels of safety required."

Let me end by stating explicitly that my aim in making these selective quotations is to encourage RISKS readers to study the full paper and debate its conclusions (preferably in that order!); as I mentioned at the outset, it is not to imply my total agreement even with those parts of the paper I have chosen to quote.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK

Article on VDT Radiation

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Wed, 22 Aug 90 11:17:35 PDT

The 8/17 issue of The Nation has an article by Herbert Kohl that describes the effect upon the industry of an article by Paul Brodeur on the hazards of VDT radiation that appeared in MacWorld. Brodeur's MacWorld article reviews the evidence on VDT radiation (a summary of what is in his book, "Currents of Death: Power Lines, Computer Terminals, and the Attempt to Cover Up Their Threat to Your Health"), then gives the results of testing ten monitors commonly used with the Macintosh. From Kohl's article:

"At twelve inches electromagnetic radiation ranged from a low of 1.11 milligauss (but was generally higher than 2) at the front of the screen to a high of 15.86 milligauss at the side of a color, high resolution monitor. (The sides and backs of monitors emit the highest levels of radiation.) They found that only at a distance of twenty-eight inches -- 'arm's length' -- was it 'sensible' to sit at the front of the screen. Four feet was their recommended distance from the sides and back."

Brodeur contends that epidemiological studies strongly suggest that levels of low-frequency electromagnetic radiation from power lines, water-bed heaters, electric blankets, and VDTs may increase risk of leukemia, brain cancer, and reproductive disorders.

In response to the MacWorld article, Apple announced that it will support the development of industry-wide safety standards for electromagnetic emissions, but argued that there is yet no scientific proof of how electromagnetic radiation affects the body.

11

✓ Terminally dumb -- substitutions

Tony Scandora 708-972-7541 &35048@ANLCMT.CMT.ANL.GOV> Wed, 22 Aug 1990 14:26:43 CDT

The Chicago Tribune, sometime around 30 July 1990, reported the following:

The computer terminals at newspapers are equipped with all sorts of dangerous buttons that should be purged from the keyboard. One is the "spell" key, which transforms poor spellers into non-spellers. Another is the "search-and-replace" key, which at a single touch can, for example, change "FBI" to "Federal Bureau of Investigation," or vice versa. The Fresno Bee in California has this technology, and because of it had to run the following correction the other day: "An item in Thursday's Nation Digest about the Massachusetts budget crisis made reference to new taxes that will help put Massachusetts `back in the African-American.' This item should have said `back in the black.'"

Tony Scandora, Argonne National Lab, 708-972-7541

[An article in the 28 July 90 Boston Globe was previously reported to RISKS by

Roger H. Goun <goun@ddif.enet.dec.com> on 28 July 90,

Rob Gross <ROSS@BCVMS.BITNET> on 1 Aug 90,

David 'Witt' <wittenberg%ultra.DEC@src.dec.com> on 6 Aug 90, among others. I finally got around to running Tony's version today, because the Globe article did not note the automated substitution capability, and it could have been just a human reedit. For those of you for whom this is a new phenomenon, RISKS has run many similar tales in the past. PGN]

✓ useful credit-related addresses

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Fri, 17 Aug 90 08:51:08 EDT

Protecting Your Credit and Your Privacy

By Simson L. Garfinkel

1. The first step to protecting your credit record is to get a copy of it. If there is invalid information on the report, have it corrected.

If you have been denied credit within the last 30 days, the credit reporting agency is obligated under the Fair Credit Reporting Act (FCRA) to provide you with a copy of your credit report for free. Otherwise, you will be required to pay \$15 for the report. (If you live in Maryland, the cost for the report is \$5; in California, \$8; and in Connecticut, \$10.)

When requesting your report, be sure to include your name, address, previous addresses for the past five years, your social security number, your signature, and a telephone number where you can be reached during the day.

In addition to your credit history, the report will include the names of

every business that has requested your report within the past two years. If you do not recognize any of the companies, someone may have obtained credit in your name.

Since each credit bureau maintains its own files, some may have errors that others do not. You should be sure to check with more than one bureau. The ``big three'' are:

TRW P.O. Box 5450 Orange, CA 92667 714-991-5100

Equifax 5505 Peachtree Dunwoody, Suite 600 Atlanta, GA 30358 404-252-1134

Trans Union Corporation Consumer Relations Dept. P.O. Box 119001 Chicago, IL 60611 312-645-6008

There are also many local credit bureaus. Bankcard holders of America, a non-profit consumer education group, publishes a ``credit-check kit'' that includes the name, address and phone numbers of legitimate credit bureaus across the country, as well as a pamphlet that explains in details your rights under the FCRA. The kit costs two dollars and is available from:

Bankcard Holders of America 560 Herndon Parkway Suite 120 Herndon, VA 22070

If you disagree with anything on your report, contact the credit bureau. The FCRA requires the bureau to reinvestigate the facts in the dispute; if you do not agree with their conclusion, you have the right to include a statement in the report with your version of the story.

2. Obtain a statement of your earnings from the Social Security Administration every two years. This will tell you if someone else is earning wages under your social security number, which can lead to many difficulties at retirement. If you suspect an error, you have three years, three months and 15 days after the mistake is made to challenge it.

To get your statement, you need to fill out a Request For Earnings and Benefit Estimate Statement card, which can be ordered by telephone from the Social Security Administration's toll free number, 800-234-5772.

3. You can ``opt-out" of direct marketing and telemarketing by having your name added to the databases maintained by the Direct Marketing Association. Write to:

Telephone Preference Service Mail Preference Service Direct Marketing Association 6 East 43rd Street New York, NY 10017 212-689-4977 ext. 369

The major credit bureaus also use their credit databases for direct marketing, and many magazines also sell their subscription lists for advertising purposes. You can write to each company that has your name and address and ask that your names not be released for marketing purposes.

4. You can get a copy of your medical information file by writing to: Medical Information Bureau
P.O. Box 105
Essex Station Boston, MA 02112
617-426-3660

The MIB will tell you if they have a file on you, but in some cases they will send its contents only to your physician or dentist. Therefore, be sure to include that person's name and address.

5. Do not permit merchants to record your credit or charge card account number on personal checks; these numbers are often transcribed and used for fraudulent purposes.

software patent issues

John Bruner <bruner@csrd.uiuc.edu> Fri, 17 Aug 90 09:07:45 CDT

Those who are concerned with the issues surrounding software patents may find the following of interest:

Pamela Samuelson, ``Should Program Algorithms be Patented?'' (``Legally Speaking'' column), Communications of the ACM, volume 33, number 8 (August 1990), pp. 23-27.

Michael Slater, ``Failings of the Patent System," (``Micro View" column), IEEE Micro, volume 10, number 4 (August 1990), pp. 96-95.

John Bruner Center for Supercomputing R&D, University of Illinois bruner@csrd.uiuc.edu (217) 244-4476

Re: compress (Sill, <u>RISKS-10.21</u>)

david paul hoyt <ZE6041@vw.acs.umn.edu> Thu, 16 Aug 90 16:28 CDT

> Not true. Although the LZW compression algorithm is transparent to users of
 > compress, as it should be, files compressed using it couldn't be uncompressed
 > by a replacement program.

Hmmm, I wonder if Unisys holds a patent on uncompressing LZW files. I'm not a patent lawyer, but it's the method of LZW compression that is patented. It seems (IMHO) that one couldn't patent the parsing of a published file format.
Or if one can, why isn't Lotus suing the pants off of everyone who 'imports' 1-2-3 files?

david paul hoyt | dhoyt@vx.acs.umn.edu | dhoyt@umnacvx.bitnet

Mew Book in Computer Ethics [See <u>RISKS-9.15</u>]

Perry Morrison MATH <pmorriso@gara.une.oz.au> 17 Aug 90 01:20:13 GMT

I'm pleased to announce the availability (like NOW) of a new book designed for teaching courses in computer ethics. It is available from MIT Press in the States and Basil Blackwell in the UK.

> Computer Ethics Cautionary Tales and Ethical Dilemmas in Computing by Tom Forester and Perry Morrison

Tom Forester, Perry Morrison, School of Computing & Information Technology, Griffith University, Queensland, Australia

[The Contents and Preface were included in full in <u>RISKS-9.15</u>. Let Perry or me know if you want a reiteration. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<seanf@scocan.UUCP> Thu, 23 Aug 90 06:15:15 EDT

>From the August 13 issue of ComputerWorld (page 7)

E-mail lawsuit cranks open privacy rights can of worms, By Jim Nash

Privacy vs Property might be a better case name for the invasion-of-privacy suit filed last week against Epson America, Inc.

The suit, born out of a personal dispute last January at Epson's Torrence, Calif., headquarters, pits those who hold electronic mail to be as inviolate

as U.S. mail against those who consider E-mail company property.

Attorney Noel Shipman filed the class-action suit in Los Angeles Superior Court on behalf of ALana Shoars, Dick Flanagan, Lee Cheaney, Glen Mosby -all former Epson employees -- and hundreds of other Epson employees who have used the company's E-mail since Auguest 1989. Shipman claimed that it was about that time that Robert Hillseth, manager of Epson's Hewlett-Packard Co. computer system, illegally tapped messages between the HP system and its external MCI Communications Corp. E-mail service.

Shipman seeks damages of \$3,000 per person for each alleged violation of a California statute barring the interception of an electronic communication without consent of all parties in the communication.

That's about all of real interest; the rest consists mostly of quotes from both sides ("we deny it," "they did it," etc.).

No risks, per se, but more the result of issues previously discussed in risks (namely, "network security," of various sorts). Sean.

Ke: Electronic house arrest units (Gong, <u>RISKS-10.22</u>)

<king@kestrel.edu> Wed, 22 Aug 90 13:34:44 PDT

Let me take a "hack" at a design for a house arrest unit.

- 0> The unit is physically attached to the detainee, looking something like a bracelet. This is in common with one of the products "out there", although not to the voice recognition unit that was the original subject of the thread.
- 1> The unit has, stored on a volatile memory chip, a supply of bit strings long enough to last the sentence. These strings need not be particularly long -- a single bit for each "string" might well suffice -- but they are set at the dispensing organization, not determined by any algorithm.

The device is built in such a manner that it can't be opened without destroying it, at least within the resources the detainee is likely to bring to bear.

- 2> At random but appropriate intervals, perhaps Poisson with lambda=ten minutes, a polling station, physically inaccessable to the detainee, broadcasts a poll signal; the bracelet broadcasts it's next bit string as stored per 1>.
- 3> The reply is received by several stations, and time delays are measured to put the detainee at the intersection of the surfaces of several ellipsoids with the polling station and each receiving

station as foci, and several hyperbolae, with each pair of receiving stations as foci.

There can be perhaps a half dozen polling stations and a half dozen receiving stations. Any attempt by the detainee to build his own repeater to simulate being where he is supposed to be is doomed to failure, because if the repeater's transmitter is at any place other than the detainee's house the intersection of the hyperbolae will turn out wrong, and if the repeater's receiver is in the wrong place the speed-of-light delay between the halves of the repeater will swell those ellipsoids whose major axes do not run along the path from the halves of the repeater.

4> There is a box at the detainee's house that listens for polls and the detainee's bracelet's response and beeps a horn if there is a failure [no response, as opposed to the wrong response]. Detainee is responsible for notifying his probation officer in case of a failure -- "Come and inspect me and bring me a new bracelet."

Can someone poke a hole in this? Seems cheap enough; 2K bytes of static RAM is a about a month's supply at one bit per poll, the detainee can't leave any device at his house to respond to polls for him because he can't open his bracelet safely, it shouldn't be all THAT expensive [and a per-bracelet cost of a few hundred or a thousand dollars does not sink the application], and yet it looks like spoofing the system involves defeating well-known physics [assuming you accept my stipulation that the detainee can't read out his RAM].

-dk

[Interesting? Overkill? Four choices among the following: A right/wrong solution to the right/wrong problem? PGN]

Proposed ban on critical computerized systems

<cameron@argosy.UUCP> Wed, 22 Aug 90 12:56:27 PDT

On page 63 of the August 1990 _World_Press_Review_:

"Unreliable Computers", by Nick Nuttall, "The Times," London

Two Australian scientists are calling for a world-wide ban on the use of computers in sensitive areas, such as hospital intensive-care wards, the nuclear-power industry, air-traffic control stations, and early-warning defense systems.

Computers are inherently flawed and too unreliable for critical tasks, say Tom Forester of Griffith University and Perry Morrison of the University of New England, both in New South Wales. In the British academic journal _Futures_, they write that computer systems cannot be designed without the threat of life-endangering malfunctions, because their very complexity makes thorough testing for errors and bugs impossible. Forester and Morrison have documented instances of death, destruction, financial loss, and mayhem caused by computers. These include patients being given fatal drug doses by malfunctioning computers; 22 fatal crashes of the Black Hawk helicopter -which flies by computer -- used by the U. S. Air Force; and 104 failures in a single day of the Los Angeles air-traffic-control computer in July, 1989.

I'd appreciate it if someone would dig up this issue of _Futures_ and post or summarize this paper.

Ke: proposed ban on critical computerized systems

<ISKS Forum <risks@csl.sri.com> [PGN]> Wed, 22 Aug 1990 14:49:34 PDT

Oddly, <u>RISKS-10.23</u> contained a note on the Ethics book by Forester and Morrison, pointing back to the Contents and Preface in <u>RISKS-9.15</u>.

As they acknowledge in their preface (<u>RISKS-9.15</u>), they drew heavily on RISKS, but they did not check all their sources. They do have a disclaimer in the book that not all of their information is guaranteed. The 22 FATAL Blackhawk crashes sounds BOGUS to me, and certainly not from RISKS. PGN

✓ Object Code Copyright Implications

&obert.Biddle@comp.vuw.ac.nz> Thu, 23 Aug 90 14:48:54 +1200

Here in New Zealand the government is reviewing the "intellectual property" laws, and several open meetings are being held to discuss the issues. I went to a recent such meeting about copyright, interested mainly in the user interface question already widely discussed on Usenet and elsewhere.

At the meeting, however, what concerned me more was the subject of "reverse engineering". Lawyers there agreed and insisted that object code be subject to copyright, and that making any "disassembled" or "uncompiled" version of the object code was making a derivative copy - and not allowed as "fair use". They argued that the only people who would wish to do this would be people wanting to get around copyright protection in creating competing programs.

I discussed this question with several of the lawyers afterward, and they explained that if you obtained a copyright protected object program, then object code was all you legally had. One lawyer suggested that would mean you could print out "ones and zeros", but nothing derived from them - they shrugged when I pointed out that "ones and zeros" notation was not inherent in object code, and so would also be a derivation. I asked how people could determine how a program might behave unless they could look at it. The lawyer suggested that it was their view that the *behaviour* of the program was sufficient for people to see how it would work.

Now there are some interesting points here.

1) If object code is copyrightable, what *exactly* is it that is subject

to the copyright? Magnetic patterns? Ones and Zeros? Source code?

2) Of course, program behaviour in the past is *not* sufficient to

determine how a program will behave in the future.

Most importantly, these people seem to be arguing that if you have (legally) an object-code program protected by copyright, and even though you *do* have the "fair use" right to execute the program, you may *not* have the right to inspect the program itself by disassembling or reverse compilation, to determine how it may work in future circumstances. This seems to me a great Risk.

Two final points:

Firstly, of course programs may be protected by other legal mechanisms which are not addressed here. But copyright is usually the minimum.

Secondly, in the meetings addressing the issues here, there was little attention paid to the rights and viewpoints of the *users* of computer programs - most discussion centred on the rights of developers. This too seems a Risk.

Robert Biddle, Computer Science, Victoria University, Wellington NEW ZEALAND

Miscover Card

Brian M. Clapper <clapper@chekov> Thu, 23 Aug 90 11:15:19 -0400

I recently received a Discover credit card and found that it boasts a 24-hour toll-free hot-line. A colleague informed me that one can call this hotline to retrieve account information from an automated system. She noted that it didn't request any identity verification, just the account number.

I called the number, and when prompted with the voice menu, selected the option that would allow me to get my account balance. I was connected with a person, not a computer. This operator requested such account verification information as my address and SSN. I figured either my colleague must have been mistaken or the Discover folks had changed their policy.

After requesting some information from the representative, I asked him whether one could obtain the same data on-line without talking to a person. He assured me that all I needed was a touch-tone phone and my account number. I asked him whether I had to verify my identify in any way -- there is no PIN associated with this card, to my knowledge -- and was told, "No."

I was a little puzzled, since I'd called from a touch tone phone, so I called back. I turns out I had made a mistake when I called the first time -- I forgot to end my request with a '#' -- and the computer assumed I was on a rotary phone and connected me to an operator. This time I pressed the '#', and the system prompted me to enter my account number. I did, and was immediately informed of my balance, available credit, previous statement balance, and current statement due date. My colleague was right: I didn't have to verify my identity in any way.

I find this odd, and more than a little irritating. First, most

bank-by-phone systems I have used require a PIN before divulging personal account data. Second, the human representative required my name, address, account number, and SSN before he would allow me to solicit information, implying that Discover has a policy of verifying an account holder's identity, but did not apply that policy to their automated system.

I don't particularly like the idea of someone being able to get that information on me merely by calling a freely advertised number and punching in my account number. Any clerk at a store where I use my card can make the call. Anyone who finds or steals my card can, as well; Discover even makes it easy by printing the number on the back of the card.

A letter complaint is in the mail...

Brian Clapper, Naval Air Development Center

* Total Knowledge about all individuals

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Wed, 22 Aug 90 13:53:40 PDT

> CANBERRA: Debt collectors believe that in the not too distant> future there will be "total knowledge" about all individuals . . .

No need to look down under or into the future for this sort of thing. Readers of misc.legal may recall a recent submission reciting a bill already passed by the Oklahoma state legislature, to take effect next January, requiring every individual to list every possession (yes, even books) and its value for tax purposes -- and requiring a physical inspection of every persons' property at least once every four years to verify the accuracy of the list.

Ke: Debt collector proposes "total knowlege" credit database

Alan J Rosenthal <flaps@dgp.toronto.edu> Thu, 23 Aug 90 17:07:55 EDT

In comp.risks ph@wyvern.cs.uow.edu.au quotes a newspaper article: >they believe banks and other lenders will have so much information that debt >collectors will be made redundant.

>"Tomorrow's credit grantor will be extending credit in a perfect market with >total knowledge of the debtor," Mr Owens asserted.

I can't believe how stupid people are sometimes when talking about the allegedly glorious future. Does he think that tomorrow's creditor's knowledge will include seeing into the future to see the debtor's circumstances at the time at which payment is required?

Sigh, it seems that only a minority of people realize that the application of technology does not automatically solve any problem.

✓ useful credit-related addresses

Henry Mensch <henry@GARP.MIT.EDU> Wed, 22 Aug 90 17:36:20 -0400

the "medical information file" that simson referred to in his article is the file that health insurers use (along with other information) to determine if an individual is insurable. if you test positive for HIV antibodies (and weren't bright enough to get tested at an anonymous test site) then your result will likely show up here...

Henry Mensch E40-379 MIT, Cambridge, MA

"Rogue Programs: Viruses, Worms, and Trojan Horses"

Gene Spafford <spaf@cs.purdue.edu> Wed, 22 Aug 90 16:17:11 EST

I just received a copy of the book "Rogue Programs: Viruses, Worms, and Trojan Horses," edited by Lance J. Hoffman. The book is published by Van Nostrand Reinhold, copyright 1990, ISBN 0-442-00454-0. The publisher's suggested list price is \$32.95, in softcover.

This book is a collection of 27 articles and book excerpts about "vandalware" on computer systems. Contributors include Len Adleman, Anne Branscomb, David Chess, Fred Cohen, George Davida, David Ferbrache, Michael Gemignani, Harold Joseph Highland, me (!), Ken Thompson, Steve White, and many others. The table of contents lists the following parts: Overview of Rogue Programs, Social and Legal Issues and Effects, Rogue Programs and Personal Computers, Rogue Programs and Networks, and Emerging Theory of Computer Viruses.

Perhaps I'm somewhat biased because I'm the author or co-author of 3 of the 27 contributions. However, I believe this is the most comprehensive collection on the topic currently available. It contains case studies, theoretical analyses, legal opinions, and step-by-step technical information. The book is valuable as both a technical reference and as a textbook around which a course can be organized. I'm sure it is going to become one of the 2 or 3 standard references in the field (the forthcoming book from ACM Press edited by Peter Denning will probably be the other biggie).

If you are interested in some of the issues involving viruses, worms and vandalware, you really should get a copy of this book and check it out. --spaf

┥ 🔶 🕨 🕤 🗹 🗤 🚀

Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 10: Issue 24



Rodney Hoffman &offman.ElSegundo@Xerox.com> Fri, 24 Aug 1990 07:58:40 PDT

Condensed from a story in the 23 Aug 90 'Los Angeles Times' by Ronald J.

Ostrow:

The General Accounting Office says that a lack of adequate computer security in the Justice Department's new "state-of-the-art" data center in Rockville, MD will permit unauthorized remote users to enter and exit the system undetected, endangering highly sensitive information such as identities of undercover operators and confidential informants.

The GAO report says that the data center is accessible over phone lines and commercial computer networks, making it vulnerable to remote users who could "introduce viruses and other disruptive software ... into vulnerable computer systems." Investigators found that contingency plans to be implemented when computer services are disrupted had either not been prepared or not tested and that no mandatory computer security training was being given all employees. They said, "Systems programmers with extensive knowledge of hardware and operating procedures had unescorted access to the data center and were capable of issuing critical computer commands that should have been limited to computer operators." Guards were not stationed and surveillance devices such as cameras or motion sensors are also lacking in some places.

The GAO blames the security weaknesses on "a lack of effective leadership and oversight by the justice management division."

A Justice Dept. public relations official said, "... we have requested additional resources from Congress for [computer security audit] and have not received them." A dept. official also said "a lot of corrective action [has already been] taken and more ... is under way."

A Step Backward (Interactive Phone Service)

Theodore Lee <lee@TIS.COM> Fri, 24 Aug 90 16:49:03 EDT

(I am sending this to both RISKS and TELECOM. I think it is germane to one or the other, perhaps even both, but I'll leave that decision up to the respective editors.)

I have been using a "pay-by-phone" service to pay bills out of my savings account for longer than I can remember; I think at least ten years. The service has been simple and straightforward: after entering your account number and PIN in response to some minimal prompting (I don't remember now whether it echoed the account number; it did not echo the PIN) you repeated a simple cycle -- (a) "enter payment code" (b) enter code, terminated by # (c) "payment code

How to Lie with Statistics [once again] (<u>RISKS-10.22</u>)

The Polymath <hollombe@ttidca.tti.com> 24 Aug 90 00:38:40 GMT

I agree with the recommendation of Huff's book, but for different reasons.

As a former statistician, I get very tired of the constant misperception that there is something inherently unreliable or evil about statistics and statistical techniques. Statistical analysis is a perfectly legitimate mathematical discipline. The techniques are well understood and they work. By definition, you can't lie with statistics without misusing those techniques.

By all means, read Huff's book to learn how and recognize when the techniques are being abused. But don't let that lead to rejecting all statistics out of hand.

As one of my former stats profs used to say: "You can lie with statistics, but not to a statistician."

Something good about Automatic Bank Tellers (Mellor, <u>RISKS-10.22</u>)

The Polymath <hollombe@ttidca.tti.com> 24 Aug 90 00:38:40 GMT

This has been standard procedure for our (Citicorp) ATMs from the first -about 15 years. The only ATMs I can think of that don't do this are some of the older Diebold machines that drop dispensed cash in a bin (a mindbogglingly bad design, IMHO). The time-delay, BTW, is usually set by the bank. Ten seconds is rather short, by our standards.

Many ATMs do similar things with cards left in card readers.

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

Ke: Something good about Automatic Bank Tellers (<u>RISKS-10.22</u>)

<tmal@computer-lab.cambridge.ac.uk> Fri, 24 Aug 90 11:38:27 +0100

In <u>RISKS DIGEST 10.22</u> Pete Mellor mentioned a useful timeout in a National Westminster Bank cashpoint machine; these machines recover money that has not been withdrawn within a short period. I have seen a similar timeout that involves the card rather than money.

I was standing in a queue at a Barclays Bank cashpoint machine behind two women who were deep in conversation. After a while the machine beeped loudly and asked whether the customer wished more time to consider the transaction. A little later it beeped again and displayed a more strongly worded message to the effect of `If you do not press a button within the next thirty seconds your card will be confiscated'. Thirty seconds later a third message appeared `Your card has been retained, please inquire inside the bank for further information'. The perspex shutter then closed over the display and keyboard; only this noise seemed able to distract the women from their conversation who then went into the bank cursing machines.

I was pleased to see that if I forget to retrieve my card it is likely to be retained by the bank rather than by a passerby. I was also pleased to note that if you want more time to consider your transaction then you can prolong the timeout. It was worth the inconvenience of waiting in the queue to see the look on their faces after losing the card.

A final thought: nobody in the queue asked the women to hurry up. Would people in other countries wait patiently or is this a British characteristic? I probably ought to have drawn their attention to the second message but I was too interested to see the behaviour of the machine.

Mark Lomas (tmal@cl.cam.ac.uk)

Ke: Electronic house arrest units (<u>RISKS-10.24</u>)

Philip L Harshman <philip@hubcap.clemson.edu> 24 Aug 90 12:46:05 GMT

The detainee doesn't have to break open the device to read out the RAM. All he has to do is poll the thing himself and record its responses. After feeding this info into a handy tabletop "device", he can go about his business. Is a big enough hole?

Philip Harshman, Clemson Universityuucp: ... !gatech!hubcap!philipbitnet: philip@clemsonphone: (803) 656-3697

Ke: Electronic house arrest units

"Jim Campbell" <jimc@ralvm11.iinus1.ibm.com> Fri, 24 Aug 90 07:25:18 EDT

In <u>Risks Digest 10.24</u>, King says that in the event of a unit failure, the parolee calls his/her probation officer and says "come and inspect me and bring me a new bracelet". Herein lies a weakness of the proposed system.

Background: About a year ago, a neighbor installed a burglar alarm system in his house. For a variety of reasons, it went off (alarmed) two or three times a week. The alarm included a rather loud bell outside his house. The first few times this happened, some of us went to see if he needed help, or see if there really was a burglar. Soon we realized that these were false alarms, and began to first ignore, then resent this intrusion. Had there been a real burglary then, no one would have paid any attention.

Back to the subject at hand. The parolee regularly calls his/her probation officer and says "come and inspect me ...". Also, the parolee should on occasion be out of range when polled, but not so far out of range that he/she can't get back in time for the parole officer to catch. Soon the parole officer begins to mistrust the system, then even ignore it. Then the parolee can begin to test the limits.

Jim Campbell

Ke: Electronic house arrest units (Gong, <u>RISKS-10.22</u>)

Amos Shapir <amos@taux01.nsc.com> 24 Aug 90 12:37:54 GMT

Just one hole, but a big one: this scheme assumes perfect reception - no echoes, interferences, etc. The urban landscape is just about the worst environment for that.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel amos@taux01.nsc.com, amos@nsc.nsc.com Tel. +972 52 522331 fax: +972-52-558322

Ke: Electronic house arrest units (Gong, <u>RISKS-10.22</u>)

Brinton Cooper <abc@BRL.MIL> Fri, 24 Aug 90 10:22:23 EDT

<king@kestrel.edu> proposes a house arrest unit, the design of which is based upon the principles of radio location. Some observations follow:

Were the radio transmissions only one-way, base-to-user, it could probably be quite inexpensive -- certainly no more difficult than personal paging services to implement.

The difficult part is that the bracelet replies. Now, instead of a few high-power transmitters to cover an urban area (say, within the "beltway" of the typical city), a large network of receivers is needed. These receivers must be connected centrally for coordination, "voting," and the ellipsoidal computations. This quickly becomes expensive, and, although it may be of lower cost than incarceration, political leaders seem to feel that "We already have a jail; we'd have to buy this system."

In addition, the urban environment provides many unintentional reflectors for radio signals. In voice communications, the receiver simply selects the strongest component and ignores the others. In a position location application, the direct component must be selected. Because of reflections and masking, the direct component may not even reach the receiver.

Also, the risk for computational and logical error seems large. I don't believe that this application is "off the shelf," so the software is an R&D project subject to the error discoveries about which we often read in this Digest.

_Brint Cooper, BRL

Ke: Electronic house arrest units (King, <u>RISKS-10.24</u>)

Brian Tompsett <bct@tardis.computer-science.edinburgh.ac.uk> Mon Aug 27 14:18:41 GMT 1990

Risks 10.24 contains a proposal for an electronic house arrest unit which is based on distance triangulations using timing over the phone lines. This method has a hole in it the size of a barn door. The problem is that one cannot rely on calls to go via a repeatable route between any two locations or at any time. The phone company may route your call in any way it chooses and at any time. It is almost impossible to distinguish phone company re-routing from hacking re-routing. Brian

Brian Tompsett. Secretary BCS Edinburgh Branch. E-mail bct@uk.ac.ed.cs.tardis. Tel: 031 554 9424 (Office) 031 441 2210 (Home) briant@uk.co.spider

Ke: Electronic house arrest units (Gong, <u>RISKS-10.22</u>)

Mike Bell <mb@sparrms.ists.ca> Mon, 27 Aug 90 10:08:38 EDT

king@kestrel.edu proposes an "uncrackable" design for a house arrest unit based on physical propogation delays for position location and a stored key string maintained in a bracelet.

Suggested improvement:

1> Store a DES cipher key in the bracelet, and send an encrypted version of a random "probe" signal. This (a) avoids having to store a very long string of "random" bits inside the unit, and (b) reduces the risk that a "forged" bracelet could produce the correct response. (If the response is only 1 bit long, I have a 50% chance of guessing it right, don't i?)

Cracking/hacking the scheme...

2> The "people system" is probably the weakest point. Convince your parole officer that the propagation of the signal is poor, and that any alarm is probably a false alarm. Do this by: heating up /cooling down the unit, static discharge, RF flooding, putting electro-magnetic shielding in parts of the house, etc. Keep calling him/her out at 3:00am because the local CB radio is inerfering with your device. Chances are this will create some flexibility in dealing with system problems (how many maintenance engineers will be on call at 3:00am?) Will they take you back into custody, replace the bracelet, or wait until 9:00am the following morning - enough time for you to commit whatever heinous crime you had in mind?

3> Use some active ECM against the *entire system*. (I'm assuming here that the half dozen transmitting/receiving stations are city wide - on grounds of cost). Try and jam or confuse the entire system for a period of time. What are "they" going to do? Check on *every* person under house arrest?

Whether either the cost/complexity of scheme or the cost/complexity of overcoming it is justified is another question...

-- Mike Bell -- <mb@sparrms.ists.ca>

Re: Electronic house arrest units (Gong, RISKS-10.22)

"Willis H. Ware" <willis@rand.org> Fri, 24 Aug 90 10:38:59 PDT

This technique is well developed within the military and is usually called TDOA - time difference of arrival. Systems exist that can listen to 10's of thousands of pulses, sort them out, calculate ground location, and report same -- and all within a very nominal size machine.

Ke: Object Code Copyright Implications (Biddle, <u>RISKS-10.24</u>)

"Willis H. Ware" <willis@rand.org> Fri, 24 Aug 90 10:38:59 PDT

I'd like to resurface an observation that I've made from time to time in various places in regard to protection of intellectual property.

A central issue that must be sorted out somewhere along the way is the essential difference between information per se and the representation of such information. Example: One's name is information; it can be represented in ASCII, as a written signature, as a spoken phrase, in Morse code, as magnetic domains, as electrical signals, as modulation on a carrier, etc.

The legal community will have to appreciate the distinction, and establish the principle within both the judicial and the legal systems. Until it does, we'll be creating laws that deal with bits and pieces of the problem and generate increasing confusion.

Willis H. Ware

Ke: Object Code Copyright and reverse engineering.

"A. Harry Williams" <ARRY@MARIST.BITNET> Thu, 23 Aug 90 23:45:01 EDT

There was an article by Pamela Samuelson in the Jan 1990 issue of IEEE Software discussing Software copying, especially as it applies to reverse engineering. While a letter from an IBM Corporate lawyer disputed the findings in the July issue, MS Samuelson made a case for it not being a violation of the copyright. It makes for interesting reading.

/ahw

✓ Object Code Copyright Implications (Biddle, <u>RISKS-10.24</u>)

Lars Poulsen <lars@spectrum.cmc.com> Fri, 24 Aug 90 04:44:35 GMT

I would agree that a decompilation of a copyrighted program is a derived work, but I would belive that deriving this for personal use is "fair use" - subject to the same limitations as the original object code.

Every time this topic comes up, I am impressed with how well the notions

of copyright law seem to agree with the field. And every time computer people discuss this with lawyers, I am disgusted with how impossible it seems to find common ground with the lawyers when it comes down to interpreting the copyright law.

>Now there are some interesting points here.
>1) If object code is copyrightable, what *exactly* is it that is subject
> to the copyright? Magnetic patterns? Ones and Zeros? Source code?
>2) Of course, program behaviour in the past is *not* sufficient to
> determine how a program will behave in the future.

I would surmise that it is the behaviour of the program that should be copyrightable. However, for practical purposes, that behaviour needs to be determined from an inspection of some representation of the algorithms. This may require decompilation.

Hence, fair use should allow you to decompile the code, but compiling it for another machine should be considered a "copy". Likewise, a transcription of the source code with every comment deleted/replaced, and every variable name changed (and possibly transliterated into a different programming language) should be considered a "copy" even if no tokens are the same.

On the other hand, I think that "look-and-feel" goes too far. The Lotus suit and the MacIntosh suit get very close the the kind of issues that belong in patent law, rather than copyrights.

If the lawyers understood the field better, would they be more likely to be "reasonable" ? Is this an issue of poor "cross-cultural" communication, or of crossed goals ? Of different perceptions of fairness ?

Lars Poulsen, SMTS Software Engineer, CMC Rockwell lars@CMC.COM

Re: copyright on object code (<u>RISKS-10.24</u>)

Gene Spafford <spaf@cs.purdue.edu> 24 Aug 90 17:08:36 GMT

I'm not a lawyer, so don't take the following as legal advice, but.... Any lawyers out there will be certain to set me straight (or try!).

The purpose of copyright is to protect the commercial interest of the copyright holder (author or publisher). A copyright on an object code version of a program is intended to prevent you from selling copies of the program. It certainly seems reasonable to say that reverse engineering the object code preserves the copyright -- trying to sell a copy of the program in any form would infringe the economic advantage of the program author/publisher, whether that copy is the object code itself, or a new version of the program derived from reverse-engineered code.

They key here is what you do with copies. If I buy a book and make ten copies of it, the problem comes about if I sell those copies or give them away to others, thus depriving the copyright holder of those sales. If I buy a computer program and make ten copies of the program that I lock up in ten different places because I am worried about loss, I have not deprived the copyright holder of additional sales as those copies are not being used, and are therefore not depriving the publisher of potential sales. (I would probably be violating the standard license that comes with most software that limits the number of backup copies that can be made, but that isn't copyright.)

Reverse-engineering the code to see what it does is a problem if I use that reverse-engineered version to sell or give away copies of the program, or use the material to write a new program incorporating part of the old one, or to make copies that I will use internally on which I do not pay copyright royalties. Those infringe the rights of the copyright holder. Translating the copy into something I find easier to read, for my own private use, does not infringe those rights.

I don't know about New Zealand (Robert Biddle's subject), but here copyright law is "enforced" in civil courts. The copyright holder needs to sue for damages and show how the copyright was abused. (There is a criminal violation of copyright, but that requires certain proof of criminal intent, etc.) If the plaintiff cannot show that any loss or damage occurred as a result of the copying, and that all use was for private purposes, I don't see that there could be a negative judgment. In all probability, the case would never even be allowed to come to trial. Also, it is unthinkable that any copyright holder would go through the aggravation and expense of pursuing such a case over private decompilation of object code.

If the law in New Zealand currently under consideration attempts to broaden copyright to prevent private copies that do not deprive the copyright holder of royalties, and if that is what the lawyers are recommending, then I would indeed be concerned.

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

Ke: Proposed ban on critical computerized systems

Pete Mellor <pm@cs.city.ac.uk> Fri, 24 Aug 90 14:54:21 PDT

In <u>RISKS-10.24</u> <cameron@argosy.UUCP> quotes:

> Computers are inherently flawed and too unreliable for critical tasks, say Tom

> Forester of Griffith University and Perry Morrison of the University of New

> England, both in New South Wales. In the British academic journal _Futures_,

> they write that computer systems cannot be designed without the threat of

> life-endangering malfunctions,...

and asks:

> I'd appreciate it if someone would dig up this issue of _Futures_ and post or > summarize this paper.

I have a copy of the paper. If anyone wants a snail-mail copy, let me have your postal address.

I may summarise it for RISKS in the next week or two if I have time.

Pete Mellor

RHC to New York Times, re: Markoff Article

<html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html><html>

Forwarded with permission.

Date: Thursday, 23 August 1990 08:24 edt From: rhcx%beta at LANL.GOV (Robert H Courtney) Subject: NYT Article To: WHMURRAY at DOCKMASTER August 19, 1990

Mr. Max Frankel, Executive Editor The New York Times 229 West 43rd Street New York, NY 10036

Dear Mr. Frankel:

Your article, "Washington is Relaxing Its Stand on Guarding Computer Security", by John Markoff, August 19, reflects a serious misinterpretation of both the intent and the probable effect of the new Presidential directive on computer security.

The new directive replaces NSDD #145, which was issued by the Reagan administration in 1984. With the authority of that older directive, and because they were not willing to accept the utterly mundane, unexciting nature of the data security problems in most agencies, the National Security Agency (NSA) distorted the data security implementations of many federal civil agencies and reduced the effectiveness of their computer security programs.

NSA's computer security efforts were oriented exclusively about the protection of classified data from disclosure to those who did not have appropriate security clearances. Their development program did not address the need for data to be complete, accurate, timely and available. They were concerned only with the confidentiality of data and wholly unconcerned about their usefulness to their proper owners.

It has been an unfortunate NSA assumption that those with appropriate security clearances can be trusted to the level of their clearances. This ignores the damage which has been done in recent years by Messrs Walker, Pelton, Pollard,

Boyce, Smith, Miller, et al, all of whom were cleared for access to the data which they delivered to those who appeared, until recently, to be the enemy. There seems to be no basis for a belief that comparable damage has been done through technically-oriented, foreign-directed penetrations of our systems containing classified data.

Fortunately, the new directive relieves the civil agencies from a requirement that they continue to accept misleading guidance in computer security from NSA. Unfortunately, it was not issued not until significant damage had already been done.

The Computer Security Act of 1987 gives the National Institute for Standards and Technology (NIST) responsibility for providing technical guidance in computer security to the civil agencies and DoD for the protection of their unclassified data. It is regrettable that NIST is very poorly funded for work in the computer security area and, at the current funding levels, cannot provide any significant amount of the technical leadership in computer security so badly needed by the civil agencies.

Only a small portion of funds previously available to NSA for computer security would permit NIST to provide the needed guidance. Whether those funds are provided or not, the new and wisely conceived directive will not result in relaxation of the security afforded data by either DoD or the civil agencies. The new directive rectifies a serious error of the previous administration and makes it probable that data security in the civil agencies will improve - not as much as it would if NIST had adequate funding and not as much as it should, but it will be improved. The contrary impression conveyed by your reporter is unfortunate.

Sincerely, Robert H. Courtney, Jr.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Pete Mellor <pm@cs.city.ac.uk> Wed, 29 Aug 90 22:40:52 PDT

>From Channel 4 news last night (Tue. 28th Aug.):

It is reported that Iraq may be deploying some of the Royal Navy's latest high-tech weaponry. Apparently this is causing US commanders to be reluctant to send aircraft carriers into the northern area of the Gulf.

The villain of the piece is the smart mine 'Stonefish', developed by Marconi Underwater Systems under contract to the Royal Navy. This little charmer is so cute it listens to the engine noise of ships passing overhead, and can tell what type of vessel is within range. It 'hides' from minesweepers, and blows the backside off anything else.

At the heart of the system is (you've guessed it!) 'highly sophisticated and classified' *software*.

The Channel 4 investigators have in their possession the 'Technical Description and Specification' of Stonefish. The cover sheet and first few pages of this document were actually shown on screen, and looked pretty authentic, with the Marconi logo and classification 'UK restricted: commercial in confidence' clearly visible.

C4's copy, however, comes not from Marconi's Watford HQ, but from a source not a million miles removed from Cardoen International, a Chilean firm (no boring restrictions on arms sales there!) described by an expert from Jane's as being specialists in the 'laundering' of military technology for the benefit of third world countries (at least, those with adequate oil revenues to pay for it). Cardoen has well-established links with Iraq.

The implication is not that Stonefish has been sold bundled to Iraq, but enough technical information is in dubious hands for the Iraqis to have a good go at building a look-alike.

Carlos Cardoen, filmed at a news conference, said that he had a very close relationship with Marconi, and some of their guys had visited him.

Marconi said 'We have no relationship with Cardoen.' and refused to be interviewed.

An expert from an outfit called something like 'Naval Weapons Review' gave it as his opinion that Iraq probably has 'a limited number of quite sophisticated mines', but implied that we shouldn't worry too much, since 'the Navy would not let a UK contractor simply hand over the software for a weapons system'.

So there you have it. Saddam Hussein is in the Stonefish plug-compatible market, but our Navies are safe provided he can't get his hands on the operating system.

All of which prompts me to wonder:-

- If the Iraqis have the software for a 'limited number' of mines, why haven't they got enough for an unlimited number?
 (Perhaps the blockade is working, and they haven't got enough floppy disks to make the copies. :-)
- 2. How does Stonefish 'hide' from a minesweeper? The cylindrical object shown in the newsreel shots doesn't look as though it is capable of crawling under a rock. Perhaps it just switches off its disk drive to stop the noise and pretends to be an oil-drum. :-)
- 3. How reliably can Stonefish identify ships by their engine noise signature? What happens if your cruiser's big ends are rattling?
- 4. Does Stonefish rely on some sort of sonar transponder to distinguish friend from foe? (Remember the Falklands helicopter!)
- 5. What are the chances that Iraq already has the software? (After all, we all know Arabs can't write programs, and software is rather difficult to smuggle through customs. :-)

- 6. The sophistication of Stonefish's recognition system argues for some kind of artificial intelligence. If it's that smart, would it know who was winning and change sides accordingly? :-)
- 7. Isn't it time that Jane's produced 'All the World's Software'?

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq. London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

✓ Computers at the Campus Bookstore

"Gary McClelland" <gmcclella@clipr.colorado.edu> 28 Aug 90 22:49:00 MDT

RISKS readers will recognize this as an old risk but it made this academic chuckle as we begin another semester. The computer at the campus bookstore prints out a tag for each required textbook indicating the course number, instructor, number of copies ordered, etc. Given that textbooks are often used by more than one course, the computer kindly prints out a cross-list of other courses using the same text. One card caught my eye with its unusually long list of cross-listings. Curious as to what textbook was so popular this term, I looked closer to see the title. Being an author I had hopes that maybe it was mine :-) Alas, the title of this very popular text was NO TEXT REQUIRED. I wonder who gets the royalties on that textbook? :-)

--Gary McClelland, U. of Colorado

Reverse Engineering - not always a copyright issue

Joe Morris <jcmorris@mwunix.mitre.org> Mon, 27 Aug 90 15:43:04 EDT

There have been several RISKS submissions recently discussing the legal status of reverse-engineering of copyrighted material. Reading them, however, one could easily conclude that copyright law is the only governing issue involved. It isn't: in fact, most of the products I've seen (both mainframe and personal computer) assert not only copyright but also contract rights. For example, IBM's FY90 GSA schedule in Special Item 132-30, section 4(a)6 (page 44) includes the item:

(6) The Government shall not reverse assemble or reverse compile the licensed programs in whole or in part.

Almost all vendors have a corresponding clause in their software license agreements, so the question of copyright law permitting reverse engineering is usually moot. Of course, we now have the issue of deciding which parts of the contract are legally enforcable. (Cf. Vault v. Quaid, in which my memory says the court held that the shrink-wrap "license contract" in PC software was unenforcable.)

Shakespeare was right: shoot all the lawyers.

re: Electronic house arrest units

"Martin Minow, ML3-5/U26 27-Aug-1990 1421" <minow@bolt.enet.dec.com> Mon, 27 Aug 90 13:02:55 PDT

It was somewhat disturbing to discover that all of the people who took time to comment on the "electronic house arrest" units focussed on the technology, and none apparently noticed that this is a safety-critical application. I.e., failure of the system may lead to the re-incarcenation of a parolee.

I would feel more comfortable if our court/prison/parole system were funded in such a way as to permit personal contact between the parolee and parole officer.

Martin Minow

Proposed ban on critical computerized systems (Cameron, <u>RISKS-10.24</u>)

Perry Morrison MATH <pmorriso@gara.une.oz.au> 28 Aug 90 04:33:45 GMT

#On page 63 of the August 1990 _World_Press_Review_:
#"Unreliable Computers", by Nick Nuttall, "The Times," London
#Two Australian scientists are calling for a world-wide ban on the use of
#computers in sensitive areas, such as hospital intensive-care wards, the
#nuclear-power industry, air-traffic control stations, and early-warning defense
#systems.

The reference is- Forester, T., & Morrison, P. Computer Unreliability and Social Vulnerability, Futures, June 1990, pages 462-474.

22 fatal crashes of the Black Hawk helicopter --#which flies by computer -- used by the U. S. Air Force

We refer to the death of 22 *servicemen* in *5* blackhawk crashes since 1982. Our reference is B. Cooper and D. Newkirk, Risks, November 1987. We didn't have a vol or issue no.

If this is incorrect, please let us know.

Perry Morrison

[The item was from <u>RISKS-5.58</u> (15 November 1987). It reappeared in in Software Engineering Notes, vol 13, no 1 (January 1988), page 7. The original source was a wire service report from 12 November 1987. The RISKS issues on the Black Hawk also included <u>RISKS-5.56</u> (9 Nov 87), 5.59 (16 Nov 87), and 5.60 (18 Nov 87). I hope that helps. PGN]

✓ Caller ID Discussion List Started

Bruce Klopfenstein <klopfens@bgsuvax.UUCP> 23 Aug 90 00:55:15 GMT

Date: Tue, 21 Aug 90 9:31:25 EDT From: Telecom Privacy List Moderator <telecom-priv-request@PICA.ARMY.MIL> To: telecom-priv@PICA.ARMY.MIL Subject: Telecom Privacy List

Hello, Everyone. The caller id list is now up and running. I have anout 35 names on it currently. The address is telecom-priv@pica.army.mil Currently, the list will not be moderated or digestified. This might change due to volume.

On Caller-Id

I believe it should be available, however the following should apply:

It should be blockable at no charge for any number.
 Name or address (or the fact it is a pay phone) should be made available.
 Actual calling number should be used not billing number.
 Under no circumstances should a third number be used shown as the actual calling number (i.e. Law Enforcement Officer dailing from one number having the id number showing up as a different number).

Optional - Show if number is listed as residental or business.

Dennis

--

Bruce C. Klopfensteinklopfens@barney.bgsu.eduRadio-TV-Film Departmentklopfenstein@bgsuopie.bitnet318 West Hallklopfens@bgsuvax.UUCPBowling Green State University(419) 372-2138; 372-8690Bowling Green, OH43403fax (419) 372-2300

[We've probably had enough on this issue in RISKS, so here is a new outlet. I've also been rejecting ATM and Electronic house arrest items unless they are particularly cogent. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Zawsuit over specification error

Martyn Thomas <mct@praxis.co.uk> Thu, 30 Aug 90 12:16:29 BST

According to Flight International (29 Aug-4 Sept, page 13), Northwest Airlines is suing CAE Electronics over a fatal aircraft crash in 1987 which Northwest claim was partly caused by inaccuracies in a CAE flight training simulator.

The crash occurred when the crew attempted to take off without deploying flaps and slats; according to the NTSB report, the crew failed to carry out the checklist, and an unexplained electrical failure caused the take-off warning system to fail to warn them.

Northwest claim that the simulator shows a warning system failure if the power fails to the warning system, whereas the aircraft system fails silently. They also claim that the crew selected go-around on the flight director, from take-off, and the result was an additional pitch-up command of 6 degrees, whereas the simulator effectively inhibits go-around from take-off. CAE says the claim is frivolous and without merit.

This claim seems to me to suggest (a) that once again, aircrew do not understand the side-effects (pitch-up, in this case) of flight-director commands (which I believe means that the systems are too complex). I also believe that the claim demonstrates the importance of formal specifications for critical systems such as simulators - on this evidence, a simulator used for crew training in emergency procedures is *itself* a safety-critical system. (Presumably it should therefore require certification in the same way as an in-flight system of equivalent criticality. Does anyone know the certification requirements for simulators?)

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

Hacking Illegal in UK - Official!

Pete Mellor <pm@cs.city.ac.uk> Thu, 30 Aug 90 19:55:57 PDT

The Computer Misuse Act came into force on Wed. 29th August 1990.

It introduces three new offences:

- 'Unauthorised access': a basic offence committed by anyone who seeks to enter a computer system knowing that the entry is unauthorised.
 Punishable by up to six months imprisonment.
- 'Unauthorised access' in furtherance of a more serious crime. Punishable by up to five years imprisonment.
- 'Unauthorised modification of computer material': Introducing viruses, Trojan horses, etc., or malicious damage to computer files.
 Punishable by up to five years imprisonment.

The act was the result of a private member's bill introduced by Michael Colvin MP (Conservative), which was supported by the government.

Extract from the Guardian, 29.08.90, p.2 [PM's comments in brackets]:

Headline: New hacking law 'too hard to enforce'

By-line: Owen Boycott

Peter Sommer [in true Grauniad style, they mis-spelt his name "Summer"], author of the Hacker's Handbook [under the nom-de-plume "Hugo Cornwall"], who opposed the need for new legislation, said yesterday he feared that doing away with the criminal damage law [??? !!! See *1 below] would make it more difficult to prosecute malevolent hackers.

"They are creating more difficulties for this offence than before," he said. The new and untried legislation might be open to challenges on the definitions of the wording of the act.

Scotland Yard's four-strong [!! *2] computer crime squad will be enlarged to cope with the extra work expected. But yesterday, one member said: "It will depend on people being aware a new crime exists, and reporting offences to us. Previously they were not certain what was a crime and what wasn't. [*3]"

During the passage of the bill, the police argued for greater powers to tap computer lines and force telecommunications companies to pursue hackers.

They were resisted by the bill's author, the Tory MP, Michael Colvin, who believes the act will prevent damage by computer hacking. [*4]

He said: "Information technology is so much a part of a company's business, that a hacker in the computer system is as bad as someone sabotaging the production line.

"It is vital companies become far more computer security conscious. Over the last five years the Department of Trade and Industry has recorded 270 computer crime cases. Only five were brought to court.

"Some have said the offence (in the act) does not go far enough, but it gives the police powers to enter and search premises...once they have gone to a judge for a warrant."

Although the estimates of the annual cost of computer crime have ranged up to [Pounds sterling] 1 billion, most is fraud committed by employees using computers for crimes that would otherwise have involved paper forgeries.

There are a few cases of hackers breaking in from systems outside companies and extracting large sums. But cases of hackers breaking into systems and damaging computer files are increasingly common.

Fears that there will be a sudden round-up of young computer enthusiasts who have been hacking are unlikely to materialise. Like almost all legislation [almost??], the Computer Misuse Act is not retrospective.

The DTI [Department of Trade and Industry] has welcomed the act, and hopes it will encourage companies to take more care over systems' security. [*5]

End of extract

Notes:-

*1 Criminal damage is an offence that has nothing to do with computing, and it has certainly not been 'done away with'. Since Peter Sommer is acutely aware of this, I suspect that the Grauniad has garbled his words. I can envisage a future prosecution involving both the offences created by the new act *and* the old offence of criminal damage (which was the charge under which Nicholas Whiteley was sent down for four months a short while ago: see <u>RISKS-10.03</u>, 10.09, 10.10). A police spokesman was quoted at the time as saying that the new act would not have made it any easier to convict Whitely. Peter Sommer has always argued that this existing offence is adequate for prosecuting a hacker who has caused actual damage. *2 Wow! Those guys are really taking this problem *seriously*!

*3 [Censored, even though disemvoweled (as in *br*dg*d or s*n*t*z*d). PGN]

- *4 Nice to meet an optimist! The plea for increased police power to intercept communications was supported by Emma Nicholson, MP, whose earlier bill failed for lack of parliamentary time See <u>RISKS-10.03</u>. It is a fact of human psychology that people are *not* deterred by a stiff penalty from indulging in a profitable or enjoyable (but illegal) activity which has a low probability of being detected. See, for example, H.J. Eysenck: "Sense and Nonsense in Psychology". Eysenck cites the cases of sheep stealing in 18th century England, which persisted at a high rate though punishable by hanging, and of his own family's flight from Nazi Germany *with* the family jewels, when removing assets (but not fleeing in its own right) was punishable by death. If you want to stop hacking, make it certain that hackers will be caught. So why do I not support Nicholson? Because I'm a pinko liberal and prefer my communications untampered with even if it slightly increases the opportunity for undetected crime.
- 5* Fat chance! If anything, it will make them more complacent. To his credit, Colvin does criticise system owners who are lax about security, and regards their slackness as a dereliction of their duty to their users (RISKS-10.03).

BTW, we await the test case with baited breath.

As for the future of hacking? Well, as someone said when prostitution was made illegal in New Orleans (or was it Paris?):

"They may make it illegal, but they'll never make it unpopular!"

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq. London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

NSA Press Release on NCSC reorganization

Jack Holleran &olleran@DOCKMASTER.NCSC.MIL> Thu, 30 Aug 90 15:56 EDT

The following is the press release approved on August 20, 1990 by the National Security Agency:

The National Security Agency (NSA) has announced that the National Computer Security Center (NCSC) will be functionally realigned to enhance its capability to respond to network and system information challenges. The NCSC was created by the Department of Defense in 1981 to provide needed emphasis on computer security and serve as a center of technical expertise.

The restructuring, which has been under consideration for some time, will serve to facilitate the integration of the Agency's communications security technical expertise and the computer security development and evaluation process to better assure systems oriented solutions to system security problems. The restructuring was prompted by increasing recognition that current user applications virtually eliminate traditional distinctions between telecommunications and information systems such that a functional merger of the communication security and computer security disciplines was necessary to effectively address network and system security issues.

The NCSC will continue to operate as a separate reporting element of NSA's Information Systems Security Directorate. Patrick Gallagher, a senior NSA official and Director of the NCSC, will be responsible for assuring that the integration of communications security and computer security technical expertise strengthens the NCSC's effectiveness in the development of criteria for and the evaluation of information systems.

Agency officials emphasized that all NCSC activities will continue and that this convergence of resources and skills from the two disciplines is intended to enhance the NCSC's ability to fulfill its responsibilities and effectively meet new challenges. These responsibilities include providing technical support to activities of the National Institute of Standards and Technology under the Computer Security Act of 1987 (P.L. 100-235). NCSC remains committed to providing this support and to fostering the availability of secure products to protect U.S. Government classified information as well as unclassified and sensitive information, to the extent such technology has application, is economically advantageous, and is consistent with the Public Law. All of the NCSC's commitments to its industry partners regarding product and system evaluation will continue to be met.

No computers on Washington State ferries

David B. Benson <dbenson@yoda.eecs.wsu.edu> Wed, 29 Aug 90 18:07:51 pdt

As the silly season draws to a close, it is time to note that the reporter quoted in the RISKS item beginning

(From The Lewiston Morning Tribune, June 30, 1990)

Associated Press

SEATTLE--The Orcas Island ferry dock, badly damaged when a state ferry rammed it, ...

was wrong regarding the following sentence:

Ferry operations superintendent Don Schwartzman said it appeared the ship's computerized power supply control system failed to respond to commands.

Followup stories confirmed what every ferry lover already knows: There are no computers on Washington State ferries. All were removed several years ago.

[Or else the superintendent did not know that the computers had been removed, as reported was going to happen way back in RISKS volume 4. PGN]

Re: Discover Card

Will Martin <wmartin@STL-06SIMA.ARMY.MIL> Thu, 30 Aug 90 14:28:31 CDT

I tried to respond to "Brian M. Clapper <clapper@chekov>" by mail, but can't find a host named "chekov" anywhere in the NIC host tables, when trying to make the address given into something replyable-to.

[He has a decidedly noncompliant mailer. That is what his mail said. Try clapper@nadc.navy.mil . PGN]

His comments on the Discover Card didn't ring a bell with me, so I dug around my own Discover Card paperwork. First off, Mr. Clapper said there was no PIN associated with the card, but not only did I receive a PIN with mine, but there was a form to fill out and send in to get another form (!) to request a specific PIN. You need the PIN to use the card in certain ATM networks to get cash. (I've never done that, by the way.)

Secondly, he said the 800 number was written on the back of the card. There is no number on the back of my Discover Card.

The Discover literature I have is full of the number 1-800-858-5588 (to call to report a lost/stolen card, etc.). I called that number just now to see if I'd get the automated interface he described, and, lo and behold, I instead get an intercept recording that says, "The 800 number you have dialled has been disconnected. No further information is available about this number." [!] I find that rather astounding -- even if Discover switched numbers, they still should have a cross-reference to the new number. The only thing that comes to mind is that Discover changed 800 carriers, and the one that has 858 doesn't want to give any business to whatever firm took over the Discover account.

I do consider it a "RISK" that the number cited in the cardholder's literature as the one to call about a lost or stolen card does not work and has no forwarding or cross-referencing to the current correct number.

I didn't bring a recent bill with me, so I don't have their current 800 number to compare with this. I found a different "customer service" number in the paperwork, too (1-800-451-4451), but it gets the same intercept recording. Glad I found this out now, rather than when I had an urgent need to call them! I'll see if I can locate a current number and update this info in case I need it sometime.

Since I couldn't try out the automated response system for Discover, I took a chance and called the number on the back of my AT&T "Universal" Card (MC version). They have one, also. I waded thru the menus and found out that they, too, do not ask for a PIN but they *do* ask for the "ZIP code of your billing address" as verification. I think that is a good compromise. I never carry the card PINs with me, nor have them memorized, since I never use the functions that require them. So this is something I *do* know and that would be at least some deterrent to a thief who has someone else's card. If he has the whole wallet, with ID and cards, though, he'll have that ZIP (probably).

Will wmartin@st-louis-emh2.army.mil OR wmartin@stl-06sima.army.mil

Re: proposed ban on critical computerized software

Al Arsenault <Arsenault@DOCKMASTER.NCSC.MIL> Thu, 30 Aug 90 17:54 EDT

While I am certainly not in favor of letting your typical computer program/ system be given full control (with no chance for override or other intervention) of safety-critical situations, I am bit disturbed by a blanket call for banning computers from being used in such environments at all. It strikes me as a little odd that no one has seemed to mention the drawbacks of such a ban.

For example, I throw out the following questions without knowledge of the answers, but hoping that those who have called for this ban have carefully thought through all of them:

(1) suppose that computers are banned from intensive care units? How many extra people are going to be needed? What is the chance of a human error occurring, with people instead of machines? Furthermore, what equipment will be used in place of certain computerized monitors? (This one hits close to home, folks. A computerized heart monitor notified Intensive Care nurses and cardiologists that my father was having a heart attack, resulting in his living five more years instead of diying then and there. The cardiologists on duty both commented that it was lucky the hospital had installed the monitors the previous week, as there was (to their knowledge) no other equipment that would have alerted them in time to save his life.)

2. If you ban computers from early warning systems (assuming that you need such beasts), what are you going to use? Do you have any idea how many extra people it would take? Or what the chance would be of an error caused by the sheer boredom of these people? Or what the chance would be that no response would be taken when needed, because of an inability to collate data in time? While I believe that letting a computer be in total charge is RISKy, to say the least, I believe that taking computers totally out of the loop would be far more RISKy.

3. If you ban computers from flight control systems, what do you do about the increased wear and tear of the electromechanical parts that replace them? What do you do about the increased strain on the pilots? Again I am not advocating letting computers have complete control of the aircraft (as I pilot myself, I certainly don't wnant that). However, I think that the tradeoffs need to be carefully considered before one advocates such an extreme measure as a total ban.

In summary, while I do NOT believe that computer hardware/software is of sufficient quality as to be trusted with the sole stewardship of human life, I DO believe that the decision as to whether or not to automate should be made after a careful analysis of the RISKS of both potential decisions, not just the RISKs of automating.

Al Arsenault Visting Professor, Computer Science U.S. Air Force Academy

[***Visiting?*** Or a Chair endowed by Col. R.Visting? PGN]



Report problems with the web pages to the maintainer



Re: Lawsuit over specification error

Pete Mellor <pm@cs.city.ac.uk> Fri, 31 Aug 90 10:14:37 PDT

Martyn Thomas in **RISKS-10.27** writes:

> ... on this evidence, a simulator used for> crew training in emergency procedures is *itself* a safety-critical system.

Safety-*related*, I would say, but not safety-*critical*. The usual definition of safety-critical is that a system failure results in catastrophe. The argument would be over how directly the catastrophe results from the failure. In this case, the 'accident chain' is fairly tenuous.

> (Presumably it should therefore require certification in the same way as an> in-flight system of equivalent criticality.

I agree that it requires certification, even though it is not safety-critical

in the strict sense. I do not think it should require to be certified to a 10~-9 maximum probability of failure per hour, as airborne safety-critical systems are, however. (This is unrealistic where software is concerned anyway.) Also 'failure' means different things in the two cases. The airborne system fails when it malfunctions and the aircraft crashes. On the simulator, one would often simulate such a 'failure' and the resulting crash, to see if the pilot could save the aircraft in those circumstances. The simulator fails when it does not faithfully mimic the behaviour of the real aircraft.

> Does anyone know the certification requirements for simulators?)

No, but I am certain they are not covered by RTCA/DO-178A, for example, which applies purely to software in airborne systems. Whether there is a section of the more general Federal Aviation Regulations which applies to ground-based ancillary systems I am not sure, but I suspect there is nothing to cover simulators, since they are not directly involved in controlling flight.

If this is the case, then the user of a simulator is at the mercy of the developer's internal quality assurance procedures.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Re: Lawsuit over specification error

Martyn Thomas <mct@praxis.co.uk> Fri, 31 Aug 90 11:47:24 BST

Peter Mellor replies to my comment in RISKS (my original lines are ">" his are ":" ...

: > ... on this evidence, a simulator used for

: > crew training in emergency procedures is *itself* a safety-critical system.

: Safety-*related*, I would say, but not safety-*critical*. The usual definition

: of safety-critical is that a system failure results in catastrophe. The

: argument would be over how directly the catastrophe results from the failure.

: In this case, the 'accident chain' is fairly tenuous.

I disagree (my comments are on the *principle*; I am not advising the lawyers in this particular case!)

Firstly, if crew are trained to react in a way which is likely to be fatal in an emergency, then the training *causes* the fatality in that emergency. This is a direct link. You cannot expect crew to do better than their training under the stress of an emergency.

Secondly, there is a class of in-flight systems which "increase crew workload", with defined failure-rate requirements. The training simulator would seem directly equivalent to these systems, in that crew might be expected to be able to overcome faulty training by cross-checking with other training and basic airmanship - but the workload could be significantly higher, and you would not expect crew to have time to react in this way in an emergency.

:

: > (Presumably it should therefore require certification in the same way as an

: > in-flight system of equivalent criticality.

Not 10⁻⁹, but some lower figure, as defined in DO-178a.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

Ke^3: Lawsuit over specification error

Pete Mellor <pm@cs.city.ac.uk> Fri, 31 Aug 90 14:52:19 PDT

I don't think that Martyn and I have a serious disagreement here.

In particular, I agree that:

> You cannot expect crew to do better than their

> training under the stress of an emergency.

and therefore I *basically* agree with Martyn when he says:

>:> (Presumably it should therefore require certification in the same way as an >:> in-flight system of equivalent criticality.

> ^^^^^

However:

As I stated previously, we are certifying different functions. With a safety-critical airborne system, we are certifying that it has a certain maximum probability of crashing the aircraft. With a simulator, we are certifying that it has a certain maximum probability of not behaving as the real aircraft behaves.

It would be unrealistic and unreasonable to demand that a simulator be certified to the same high reliability (1 - 10⁻⁹) as a critical airborne system.

It is in any case impossible to certify any system containing software to a reliability of $(1 - 10^{-9})$, even if it *is* a critical airborne system.

RTCA/DO-178A ('Software Considerations in Airborne Systems and Equipment Certification') does *not* define any reliability figures. It is merely a set of guidelines defining quality assurance practices for software. Regulatory approval depends upon the developer supplying certain documents (e.g., software test plan, procedures and results) to show that the guidelines have been followed.
I will return to this last point at length in the near future. Watch this space.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Computer Unreliability and Social Vulnerability: synopsis

Pete Mellor <pm@cs.city.ac.uk> Fri, 31 Aug 90 12:44:12 PDT

Synopsis of: Forester, T., & Morrison, P. Computer Unreliability and Social Vulnerability, Futures, June 1990, pages 462-474.

Abstract (quoted):

Many have argued that industrial societies are becoming more technology-dependent and are thus more vulnerable to technology failures. Despite the pervasiveness of computer technology, little is known about computer failures, except perhaps that they are all too common. This article analyses the sources of computer unreliability and reviews the extent and cost of unreliable computers. Unlike previous writers, the authors argue that digital computers are inherently unreliable for two reasons: first, they are prone to total rather than partial failure; and second, their enormous complexity means that they can never be thoroughly tested before use. The authors then describe various institutional attempts to improve reliability and possible solutions proposed by computer scientists, but they conclude that as yet none is adequate. Accordingly, they recommend that computers should not be used in life-critical applications.

Synopsis of paper:

The paper is introduced by a series of examples of disasters, some to do with communications kit and some with computers, covering external causes and internal system failures, and accidental and malicious actions, e.g. sabotage of telephone cables in Sydney in Nov.'87, fire in Setagaya telephone office (Japan) in Nov.'84, overwriting of Exxon's files relating to the Alaskan oil spill in July '89.

The vulnerability of society to such failures is further underlined by a discussion of 'The problem of computer unreliability: sources extent and cost'. System failures can be caused by external factors (flood, fire, etc.), and human error or misuse, but many more are due to computer malfunction, which can be classified as hardware or software failure. Hardware failures are usually due to failures of computer chips, e.g. the SAC false alert in June '80. However most computer malfunctions are due to software failure. Many examples are given of accidents, loss and disruption due to software failure in military, space, civilian air traffic control, medicine, and finance, and of cost overrun during software development. Famous examples cited are the loss of Mariner 18 and the Bank of New York disaster in Nov.'85. Reports from Price Waterhouse and Logica are mentioned as stating that software failure

costs UK industry US\$900 million a year. Finally the case of Julie Engle, who died after an overdose of painkiller was prescribed by an automated dispensing machine, is reported as an example of how a fairly simple AI system can fail with disastrous consequences, and the authors ask what could happen with the really complex systems now envisaged.

In discussing 'Why computers are so unreliable', the authors complain that previous studies have failed to highlight hardware or software failure as a source of system malfunction. Their contention is that computers are inherently unreliable because they are prone to catastrophic failure, and they are too complex to be tested thoroughly. The Therac-25 and Blackhawk helicopter accidents are given as examples of catastrophic failure. Digital computers are discrete state devices, with billions of possible internal states, each of which is a potential error point. Each internal state depends on the previous one, and if any execution of an internal state results in an 'incorrect' state, sudden erratic behaviour or total failure will result. In contrast, although analogue devices have infinitely many states, most of their behaviour is *continuous*, so that there are few situations in which they will jump from working perfectly to failing totally. Furthermore, the enormous number of possible internal states in a discrete computer system means that it is impossible to know or predict, and hence impossible to test, them all. Attempts at repair of computer systems often introduce more errors. Bug-free programs cannot be guaranteed, as illustrated by lack of software warranties, or explicit disclaimers.

'What are computer scientists doing about it?': Computer system reliability has traditionally been assessed by estimating the probability that hardware or software will fail based on statistics of failures observed over operating time. This confirms that programming is still a 'black art', a creative but hit and miss activity undertaken in an unregulated fashion by people of whom no minimum standard of education is required. This is likely to change following the publication of the draft defence standard 00-55 by the MoD in the UK in May 1989. The DoD in the US are not doing anything similar, though the International Civil Aviation Organisation is planning to go to formal methods. The improvement of software has until now depended upon 'software engineering' under four headings:

- a) structured programming and associated HOLs,
- b) programming environments providing version and modification control,
- c) program verification and derivation (proof of correctness of code and intermediate specifications respectively), and
- d) human management.

a) and b) will not give the order of magnitude improvement required.
c) can only be applied to small programs, and is better described as 'proof of relative consistency' rather than 'proof of correctness', since it takes no account of situations not foreseen in the specification.

Conclusion (quoted):

We are therefore forced to conclude that the construction of software is a complex and difficult process and that existing techniques of software engineering do not as yet provide software of assured quality and reliability. In the case of large, complex systems to which we entrust major social

responsibilities and sometimes awesome energies, this is extremely worrying. Nor is the situation likely to improve in the short term: computer unreliability will remain a major source of social vulnerability for some time to come. Accordingly, we recommend that computers should not be entrusted with life-critical applications now, and should be only if reliability improves dramatically in the future.

Given the evidence presented here, several ethical issues also emerge for people in the computer industry. For example, when programmers and software engineers are asked to build systems which have life-critical applications, should they be more honest about the dangers and limitations? Are computer professionals under an obligation if a system fails: for example, if a patient dies on an operating table because of faulty software, is the programmer guilty of manslaughter, or malpractice, or neither? What is the ethical status of existing warranties and disclaimers? How is it that the computer industry almost alone is able to sell products which cannot be guaranteed against failure?

These are the kinds of questions that should be raised with governments, computer purchasers and the wider public as a matter of urgency, because computer vendors and the software industry themselves are most unlikely to publicize the serious shortcomings of their products.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Computer Unreliability and Social Vulnerability: critique

Pete Mellor <pm@cs.city.ac.uk> Fri, 31 Aug 90 21:03:31 PDT

Ref.: Forester, T., & Morrison, P.: "Computer Unreliability and Social Vulnerability", Futures, June 1990, pages 462-474.

The original item (<u>RISKS-10.24</u>), taken from the August 1990 _World_Press_Review, was a very short and over-simplified summary of this paper, and included one gross inaccuracy that the authors were not guilty of (22 fatal Blackhawk helicopter crashes, instead of the true figure of 5 crashes resulting in 22 deaths), as Perry Morrison himself pointed out in <u>RISKS-10.26</u>.

In my previous mailing, I provided what I hope is a fair synopsis of this paper, accurately representing the views of the authors, and without allowing my own opinions to intrude. (I quoted the abstract and conclusions in full.)

The following is my own reaction to the paper:-

The authors are basically on the side of the angels, and I agree with a lot of what they say. (They also cite one of my own articles, so appealing to my vanity and making it even more difficult for me to be critical! :-) However, bearing this in mind, I would like to raise some criticisms.

An enormous number of CAD/CAM incidents (Computer Aided Disaster/Computer

Assisted Mayhem :-) are retold. Some of these are not directly relevant to the authors' main point, which is that the activation of faults, unintentionally introduced into their design, is now one of the most important reasons for the failure of complex hardware/software systems (a point with which I entirely agree). They include deliberate sabotage of hardware, malicious alteration of data, accidents (e.g., fire) external to the system, and physical hardware component failure (e.g., broken wires). In considering the social impact of the failure of complex systems, such causes must not be ignored, but the authors confuse the issue by not distinguishing these events clearly from failures due purely to design faults.

The incidents could have been more clearly described by classifying them according to:

- application area (military, banking, etc.),
- cause (code fault, bad specification, hardware failure, interference, etc.),
- effect (system crash, data corruption, spurious signal, etc.), and
- cost (\$5 million, 22 lives, etc.).

The authors do not make it clear initially which of two different meanings of 'catastrophic' they intend:

a) sudden and unpredictable, 'anything can happen', andb) having appalling consequences.

The first is a classification of the effect (which I prefer to call a 'wild failure' to avoid confusion), and the second is a measure of the cost. For example, when arguing that computers are inherently unreliable because they are prone to 'catastrophic failure', they quote the Blackhawk example. The cause of this series of accidents was eventually traced to electromagnetic interference, as the authors state. While it is probably true that only a *digital* fly-by-wire system would exhibit a wild mode of failure in response to EMI, it is not until half-way down the next page, where the authors point out that digital systems have far more discontinuities than analogue systems, that it becomes clear that they are using 'catastrophic' in sense a), and not in sense b).

The authors are right to claim that computer systems are too complex to be tested thoroughly, if by this they mean 'exhaustively'. It is apparent from their example of a system monitoring 100 binary signals that they do mean this. The argument, and the arithmetic supporting it, are unconvincing, however. It is not generally true that a different path through a program will be executed for every possible combination of inputs, therefore the derivation of 1.27 x 10^34 internal states (2^100 or 1.27 x 10^30 input combinations, multiplied by an arbitrarily assumed 10^4 possible paths) is not valid. On the other hand, knowing that execution is along a given path is insufficient. *Where* one is on the path would also affect the internal state. There may be *more* than 1.27 x 10^34 internal states! The problem is that 'internal state' is not defined.

Exhaustive testing in this sense is well known to be impossible. Even in modestly complex systems one can only test a representative sample of inputs. Provided the selected sample is realistic, one can, however obtain a reasonable degree of confidence that a reliability target has been reached, but *only if the target is not too high*.

Later in this argument, there is further confusion between two types of 'modification':

i) changes to a system to simulate exception conditions during testing, andii) changes to a system to correct faults found in test or operation.

The authors slip from i) to ii) without, apparently, being aware of it. As a result, there is a non-sequitur, although the final points, that attempts to remove faults have a high probability of introducing other faults, and that guaranteed bug-free programs are impossible, are quite correct.

In the section on 'What are computer scientists doing about it?' there is another non-sequitur (quoted text prefixed by '>'):

> Like many computer scientists, he [Peter Mellor] advocates the application
> of statistical principles to software quality, so that, for example, it may
> be more acceptable to have many infrequent bugs rather than a small number
> of very frequent ones.

This point was originally made by Bev Littlewood. I still advocate it, but it needs clarifying. We value a system for the function it performs, and therefore we are interested in its reliability, defined as: the probability that it will not fail (i.e. deviate from its required function) for a given period of operation under given conditions. (The authors quote this definition, but omit the 'not' - obviously a typo! :-) The program with many bugs, each of which causes failure infrequently, may be much less likely to fail than one with few bugs, each of which causes failure frequently. In that case it will be more acceptable, since it is more reliable. The only 'principle' involved here is that reliability is an important attribute of software quality, which the authors also affirm. They continue:

> This merely confirms the view that programming is a 'black art' rather than> a rigorous science - a highly creative endeavour which is also hit and miss.

Does it? Why?? I see no logical connection here at all. "We cannot control what we cannot measure" [de Marco]. If we wish to control software development to achieve more reliable systems, we must begin by being able to measure reliability. To make such measurements using sound statistical techniques on well-defined data moves programming away from being a 'black art' and towards being an engineering discipline.

If the authors are pointing out that this kind of 'black-box' statistical reliability assessment gives no guidance before development as to what effect particular design methods will have on reliability, I agree, but we must be able to measure first, in order to build up a body of experience regarding their effect.

Anyway, end of whinge. I agree with much of what the authors say, particularly regarding the inability of current methods to deliver ultra-reliable software. Ultra-reliability, of the order $1 - 10^{-9}$, is also impossible to assess. (If the failure rate is high enough to be measured, then it is too high!) For many applications, however, modest reliability is sufficient, and this can be both

achieved and measured right now. The moot point is whether the authors' main conclusion is too strong: that computers should not be used where life is at stake.

At which point, I throw the motion open for debate.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Copyright Policy (reply to Gene Spafford)

Daniel B Dobkin <dbd@marbury.gba.nyu.edu> Fri, 31 Aug 90 14:28:19 EDT

[I acknowledge this is not the best forum for this, but there is a RISK, far more evident on other newsgroups, when people make sweeping statements about the law based on popular misconceptions. There is another RISK inherent when judges have to make decisions on technical matters without understanding the technology -- and when those decisions are based on arguments made by lawyers who don't understand the technology, either.]

First, the disclaimer: I'm not a lawyer, either, but as a full-time programmer and part-time law student (sorry), I felt compelled to respond to Gene Spafford when he wrote,

The purpose of copyright is to protect the commercial interest of the copyright holder (author or publisher).

Don't take what I say as legal advice, either; it's an explanation of the policy underpinnings of copyright, as I understand them:

The purpose of copyright is NOT to protect the commercial interest of the copyright holder, author, publisher, artist, or anything else. Its sole purpose is to promote innovation and creativity; granting the author/artist a limited monopoly interest (exclusive rights for some definite period), it is reasoned, will encourage people to be creative and society will reap the benefits.

To a lot of people this sounds like the sort of semantic quibbling (1) which doesn't mean much; and (2) for which lawyers typically overcharge. (It sounds that way to me at times.) Please think about it for a moment: there is really a world of difference between the two. The one can encourage lawsuits based on, say, "software look and feel", while the other has great potential to limit them.

\dbd, Stern School of Business, New York University

Re: Discover Card

Brian M. Clapper <clapper@NADC.NADC.NAVY.MIL> Fri, 31 Aug 90 09:19:26 -0400

Will Martin points out that the card does come with a PIN. He is correct; I found that out after I sent my message. I apologize for the error. However, one does not need a PIN to access the on-line service I previously described.

Also Mr. Martin mentions that his card has no 800 number on the back. Quite possible. My card is brand new. The number I dialed was 1-800-347-2683. Discover's mnemonic for this same number is 1-800-DISCOVER. That number (in both incarnations) is imprinted on the back of my card, along with the legend "24-HOUR SERVICE".

Brian Clapper, clapper@nadc.navy.mil

P.S. My apologies for any problems our mailers caused. We're slowly switching to a new set-up, and we sometimes have trouble with sendmail's oh-so-friendly address rewriting rules.

[Join the Club. PGN]

Ke: Discover card...

Gordon Keegan &145GMK@UTARLG.UTARL.EDU> Fri, 31 Aug 90 10:44 CDT

Some time ago I received notification from Discover that there was now an 800 number available with automated account information available. It's 1-800-DISCOVER (800-347-2683). The computer on the other end has you key in your account number followed by the *#* key. No PIN is required for this. You only need the PIN if you are getting a cash advance at an ATM.

The 858-5588 number has been inactive for about a year now.

Gordon Keegan, U.Texas, Arlington c145gmk@utarlg.BITNET THEnet UTARLG::C145GMK UUCP: ...!{ames,sun,texbell,uunet}!utarlg.arl.utexas.edu!c145gmk



Report problems with the web pages to the maintainer



What is "safety-critical"?

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Fri, 31 Aug 90 18:08:40 -0700

<u>RISKS-10.28</u> was certainly provocative. I do not want to enter into the basic argument, but I would like to comment on a couple of statements that appear incorrect to me.

Peter Mellor writes:

>Safety-*related*, I would say, but not safety-*critical*. The usual >definition of safety-critical is that a system failure results in >catastrophe.

System safety engineers in the textbooks I have read do not define "safety-critical" in terms of catastrophic failure. They use "hazards" and the ability to contribute to a hazard. A safety-critical system or subsystem is one that can contribute to the system getting into a hazardous state. There are very good reasons for this, which I will attempt to explain.

Accidents do not usually have single causes -- most are multi-factorial. We usually eliminate the simpler accident potentials from our systems which only leaves multi-failure accidents. The basic system safety goal is to eliminate all single-point failures that could lead to unacceptable consequences and minimize the probability of accidents caused by multi-point failures. Using Pete's definition, there are almost NO systems that are safety critical including nuclear power plant and air traffic control systems because we rarely build these systems so that a single failure of a single component can lead to an accident. That the failure of the whole nuclear power plant or air traffic "system" is an accident is tautological -- what we are really talking about are failures of components or subsystems of these larger "systems" like the control components or the simulators (in this case).

The term "safety-related" seems unfortunate to me because it is too vague to be defined. Some U.S. standards talk about "first-level interfaces" (actions can directly contribute to a system hazard) or "second-level" (actions can adversely affect the operation of another component that can directly contribute to a hazard). Another way of handling this is to talk about likelihood of contributing to a hazard -- with the longer chains having a lower likelihood. But I would consider them all safety-critical if their behavior can contribute to a hazard -- it is only the magnitude of the risk that differs. I have a feeling that the term "safety-related" is often used to abdicate or lessen responsibility.

There is a very practical reason for using hazards (states which in combination with particular environmental conditions have an unacceptable risk of leading to an accident). In most complex systems, the designer has no control over many of the conditions that could lead to an accident. For example, air traffic control hazards are stated in terms of minimum separation between aircraft (or near misses) rather than in terms of eliminating collisions (which, of course, is the ultimate goal). The reason is that whether a collision occurs depends not only on close proximity of the aircraft but also partly on pilot alertness, luck, weather, and a lot of other things that are not under the control of the designer of the system. So what can the designer do to reduce risk? She can control only the proximity hazard and that is what she does, i.e., assumes that the environment is in the worst plausible conditions (bad weather, pilot daydreaming) and attempts to keep the planes separated by at least 500 feet (or whatever, the exact requirements depend on the circumstances).

When assessing the risk of the air traffic control system, the likelihood of the hazard, i.e., violation of minimum separation standards, is assessed, not the likelihood of an ATC-caused accident. When one later does a complete system safety assessment, the risk involved in this hazard along with the risk of the other contributory factors are combined into the risk of a collision.

Why does this push my hot button? Well, I cannot tell you how many times I have been told that X system is not safety-critical because it's failure will not cause an accident. For example, a man from MITRE and the FAA argued with me that the U.S. air traffic control software is not safety critical (and therefore does not require any special treatment) because there is no possible failure of the software that could cause an accident. They argued that the software merely gives information to the controller who is the one who gives the pilot directions. If the software provides the wrong information to the controller, well there was always the chance that the controller or the pilot could have determined that it was wrong somehow. But an ATC software failure does not necessarily result in a catastrophe so it is not safety critical (as defined above). Perhaps this argument appeals to you, but as a person who flies a lot, I am not thrilled by it. As I said, this argument can be applied to EVERY system and thus, by the above definition, NO systems are safety-critical.

Again, there may be disagreement, but I think the argument has been pushed to its absurd limit in commercial avionic software. The argument has been made by some to the FAA (and it is in DO-178A and will probably be in D0-178B) that reduction in criticality of software be allowed on the basis of the use of a protective device. That is, if you put in a backup system for autoland software, then the autoland system itself is not safety critical and need not be as thoroughly tested. (One could argue similarly that the backup system is also not safety-critical since it's failure alone will not cause an accident -- both of them must fail -- and therefore neither needs to be tested thoroughly. This argument is fine when you can accurately access reliability and thus can accurately combine the probabilities. But we have no measures for software reliability that provide adequate confidence at the levels required, as Pete says). The major reason for some to support allowing this reduction is that they want to argue that the use of n-version software reduces the criticality of the function provided by that software (none of the versions is safety critical because a failure in one alone will not lead to an accident) and therefore required testing and other quality assurance procedures for the software can be reduced.

>With a safety-critical airborne system, we are certifying that it has >a certain maximum probability of crashing the aircraft.

Actually, you are more likely to be certifying that it will not get into (or has a maximum probability of getting into) a hazardous state from which the pilot or a backup system cannot recover or has an unacceptably low probability of recovering. The distinction is subtle, but important as I argued above. Few airborn systems have the capacity to crash the aircraft by themselves (although we are heading in this direction and some do exist -- which violates basic system safety design principles).

>RTCA/DO-178A ('Software Considerations in Airborne Systems and Equipment >Certification') does *not* define any reliability figures. It is merely a >set of guidelines defining quality assurance practices for software. >Regulatory approval depends upon the developer supplying certain documents >(e.g., software test plan, procedures and results) to show that the >guidelines have been followed.

There is currently an effort to produce a DO-178B. This will go farther than 178A does. For one thing, it is likely to include the use of formal methods. Second, it will almost certainly require hazard-analysis procedures. If anyone is interested in attending these meetings and participating, they are open to the public and to all nationalities.

>From Pete Mellor's description of the Forrester and Morrison article:
>This is likely to change following the publication of the draft defence
>standard 00-55 by the MoD in the UK in May 1989. The DoD in the US are
>not doing anything similar, though the International Civil Aviation
>Organisation is planning to go to formal methods.

Depends on what you mean by similar. The DoD, in Mil-Std-882B (System Safety) has required formal analysis of software safety since the early 80s. MoD draft defense standard 00-56 requires less than the equivalent DoD standard. There has been a DoD standard called "Software Nuclear Safety" that has been in force for nuclear systems for about 4-5 years. And there are other standards requiring software safety analysis (e.g., for Air Force missile systems) that were supplanted by 882B. 882B is likely to be replaced by 882C soon -- and the accompanying handbooks, etc. do mention the use of formal methods to accomplish the software safety analysis tasks.

nancy

***** Re: Computer Unreliability and Social Vulnerability

David Gillespie <daveg@csvax.cs.caltech.edu> Fri, 31 Aug 90 21:41:05 -0700

I think one point that a lot of people have been glossing over is that in a very real sense, computers themselves are *not* the danger in large, safety-critical systems. The danger is in the complexity of the system itself.

Forester and Morrison propose to ban computers from life-critical systems, citing air-traffic control systems as one example. But it seems to me that air-traffic control is an inherently complicated problem; if we switched to networks of relays, humans with spotting glasses, or anything else, ATC would still be complex and would still be prone to errors beyond our abilities to prevent. Perhaps long ago ATC was done reliably with no automation, but there were a lot fewer planes in the air back then. If it was safe with humans, it probably would have been safe with computers, too. As our ATC systems became more ambitious, we switched to computers precisely because humans are even less reliable in overwhelmingly large systems than computers are.

The same can be said of large banking software, early-warning systems, and so on. There's no question that computers leave much to be desired, or that we desperately need to find better ways to write reliable software, but as long as the problems we try to solve are huge and intricate, the bugs in our solutions will be many and intricate. Rather than banning computers, we should be learning how to use them without biting off more than we can chew.

-- Dave

Kisks of selling/buying used computers

<pereira@icarus.att.com> Sat, 1 Sep 90 14:27:27 EDT

A 8/31/90 Associated Press newswire story by AP writer Rob Wells, entitled "Sealed Indictments Accidentally Sold as Computer Surplus," describes how confidential files from a federal prosecutor in Lexington, KY, were left on the disks of a broken computer sold for \$45 to a dealer in government surplus equipment. The files included information about informants, protected witnesses, sealed federal indictments and personal data on employees at the prosecutor's office. The Justice Department is suing the equipment dealer to return the computer and storage media and reveal who bought the equipment and who had access to the files.

The government claims that a technician for the computer's manufacturer tried to erase the files, but since the machine was broken he could not do it with the normal commands, and had instead to rely on what the AP calls a ``magnetic probe'' (a degausser?) which apparently wasn't strong enough to to the job.

The dealer complains that the FBI treated him rudely and tried to search his premises without a warrant; the Justice Department argues that the dealer hasn't been helpful and could get at the files. The dealer denies he has done so.

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

[One of the earlier classics was related in <u>RISKS-3.48</u>, 2 Sep 86: "Air Force puts secrets up for sale", in which thousands of tapes containing Secret information on launch times, aircraft tests, vehicles, etc., were auctioned off without having been deGaussed. PGN]

Accidental disclosure of non-published telephone number

Peter Jones <AINT@UQAM.bitnet> Fri, 31 Aug 90 16:27:12 EDT

The following appeared on a recent mailout from the Bell Canada telephone company. It's probably about time to repeat this warning, even if it has already appeared on the list:

"If you have a non-published telephone number, please keep in mind that if someone else uses your phone to make a collect call or to charge a call to another number, your number will appear on the statement of the person billed for the call. This is necessary because the customer being billed must be able to verify whether or not he or she is responsible for the charge."

Peter Jones UUCP: ...psuvax1!uqam.bitnet!maint (514)-987-3542 Internet: MAINT%UQAM.bitnet@ugw.utcs.utoronto.ca



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Karl Lehenbauer <karl@sugar.hackercorp.com> 3 Sep 90 11:18:30 CDT (Mon)

In the September 10, 1990 issue of Business Week, a sidebar to an article about problems at Universal Studios Florida ("MCA May Have Created A Monster") is about high-tech amusement park rides. The cavalier attitude toward risks is startling.

The article reports that "bigger thrills are needed to lure a jaded generation raised on dazzling movie special effects" and that, consequently, Universal Studios spent over \$200 million for rides such as "a giant robotic shark that attacks a boatload of tourists, a three-story animated King Kong, and a bone-jarring imitation earthquake." The article also notes that other theme-park operators, including of course Walt Disney Co., have "joined the race for "animatronics," robots, and other computerized contraptions."

Yet as the bugs plaguing Universal show, technology has its price. Says Joseph B. McHugh, vice-president of Ride & Show Engineering Inc., which made the Jaws and Earthquake rides: "The complexity of the systems means there are more components that can shut a ride down."

The scariest prospect for a park operator is a Jaws that doesn't bite. And all it takes is one software bug. At Universal, the trick is to synchronize a moving tram and an animated shark or gorilla that runs on a fixed program. "If they're not coordinated exactly, they run into one another and parts get bent," says Q. David Schweninger, chief of Sequoia Creative Inc., Kong's creator. Universal's rides are "way out in front of everyone else," he says. "The price is that you're going to have teething problems."

Later, the sidebar quotes Schweninger as saying "There are lessons to be learned here," and adding that ride makers *may* insist on more shakedown time before new rides open.

But none of this is likely to halt the shift to high-tech rides, which promise more safety and eat less real estate. Changing demographics also favor gentler high-tech rides over old-style gut-wrenchers such as roller coasters.

The article concludes by pinpointing the Disney Star Tours ride in 1987 as the first of the new wave of participatory rides and that ride makers are working on dozens of variations of the simulator ride for theme parks, casinos and special theaters.

Although it's reasonable to assume gentler rides would be safer than "oldstyle gut-wrenchers," the claim seems to be that high-tech makes the rides safer, which the rest of the article seems to refute. Oh well.

uunet!sugar!karl Usenet access: (713) 438-5018

* Arabian heat causing problems with US weapons computers

Jon Jacky <ON@GAFFER.RAD.WASHINGTON.EDU> Tue, 4 Sep 1990 10:35:49 PDT

Here are excerpts from a story in THE SEATTLE TIMES, Sept 3 1990, p. A8:

US TROOPS ALREADY UNDER ATTACK FROM SUN AND SAND by Molly Moore, Washington Post

... Patriot missiles, which are to protect critical military sites from attack

by Iraqi Scud-B missiles and attack planes, are controlled by computer equipment housed in air-conditioned vans. But the heat is so intense on each van's metal shell that it raises the temperature inside.

"Every now and then there is a glitch that makes the (radar) scope look blank," said one missile technician. He said in an attack, the computers are supposed to override any radar screen malfunction or other problem that might hinder a human operator, and track the incoming missile on their own. ...

... If the A-10 attack plane fights Iraqi tanks, it will depend on cylindrical pods under its wings to jam the signals of enemy air defenses. But weapons loaders here said the heat renders the jammers useless after about one hour of operation. A typical sortie against hostile tanks would likely require far more than an hour's protection ...

- Jon Jacky, University of Washington, Seattle jon@gaffer.rad.washington.edu

Forwarding: Stonefish mine

&ichard_Busch.sd@Xerox.com> Tue, 4 Sep 1990 10:03:21 PDT

Chaz Heritage has requested that I forward the following as a candidate for inclusion in the Risks Digest. He is apparently unable to get mail to you directly.

richard

From: chaz heritage:wgc1:RX Sender: chaz heritage:wgc1:rx Subject: Stonefish mine Date: 3-September-90 (Monday) 4:34:36 PDT

In RISKS-FORUM Digest Wednesday 29 August 1990 Volume 10 : Issue 26 Pete Mellor asks a number of questions about the Stonefish mine which may be possessed by Iraq:

>1. If the Iraqis have the software for a 'limited number' of mines, why haven't they got enough for an unlimited number?

To the best of my knowledge each Stonefish is intended to have a unique identity to allow selective arming or disarming. Therefore the software installed in each mine will be slightly different from the others'. It is likely that Stonefish's software is in ROM, and not loaded into RAM from floppies as Mr. Mellor seems to suggest. Manufacturing more ROMs, even if one knows how to assign new identities, would require a ROM-burner and a supply of blanks. The sort of ROMs used are possibly 'strategic goods' and not available directly to Iraq, nor, perhaps, to Cardoen.

>2. How does Stonefish 'hide' from a minesweeper?<

Gee, that sure is classified!

Minesweepers can detect mines by a number of methods, to each of which countermeasures may be available. Sonar, for example, may be spoofed by returning an amplified signal, too big for a mine (so it looks like a whale or wreck, perhaps?). Countermeasures may exist against magnetic anomaly detection, but these are not disclosed in the unclassified literature (since MAD is used to detect SSBNs this is hardly surprising). There may well be other countermeasures included in Stonefish's suite.

>3. How reliably can Stonefish identify ships by their engine noise signature?

What happens if your cruiser's big ends are rattling?<

The noise signature is mainly a function of the screw design, which is why there was so much fuss over the Japanese selling the USSR some CNC machining equipment capable of manufacturing low-noise screws. A ship trying to avoid acoustic detection will proceed slowly and as quietly as possible, but it cannot conceal the characteristic noise caused by screw cavitation at any speed above a knot or two.

>4. Does Stonefish rely on some sort of sonar transponder to distinguish friend from foe?

I imagine not, since if the mine were to transmit sonar in order to trigger transponders located on friendly ships then it would render the mine very susceptible to detection and countermeasures.

> 5. What are the chances that Iraq already has the software?<

100% chance of posessing the basic software if they possess the originally issued mines. Each mine would be supplied with it. Reverse-engineering it is probably a matter of copying a number of unusual boards and devices, and would depend upon posessing at least one working example and sufficient parts. Circuit boards used in weapons systems are often of unusual shape and construction and replication of them would probably not be particularly easy.

The target-recognition software, on the other hand, would probably consist of digitised acoustic samples for comparison with the signature of the target. If the mines were to be used against US or UK warships then samples of their signatures would be required. These would probably not be forthcoming. Any type of ship an example of which had been sold to Iraq might possibly be at risk (assuming the Iraqis to possess the sampling apparatus and the ability and time to use it), as might any types possessed by navies considered at any time to be hostile to the UK Royal Navy.

> 6. The sophistication of Stonefish's recognition system argues for some kind

of artificial intelligence. If it's that smart, would it know who was winning and change sides accordingly?<

Personally I wouldn't consider Stonefish to be an AI. I don't think the problem posed is much of a risk to Stonefish operators....

>7. Isn't it time that Jane's produced 'All the World's Software'?<

Yes, but it would be a far slimmer volume than their usual anti-bookshelf masterpieces (I had to get rid of all my old ones before my upstairs bedsit suddenly turned into a downstairs bedsit). I don't honestly think enough information would be disclosed to make it worthwhile.

>The implication is not that Stonefish has been sold bundled to Iraq, but enough technical information is in dubious hands for the Iraqis to have a good go at building a look-alike<

Personally I wouldn't back them to do it. If I were a naval commander I should consider the threat of anti-ship missiles fired from the air or from the Kuwaiti islands against targets acquired by aircraft possibly still within Kuwaiti airspace to be a greater threat than that of Iraq managing to copy a sophisticated underwater weapons system to a deadline.

If, on the other hand, Carlos Cardoen is telling fibs (which would not perhaps be entirely out of character) then it's possible that he's sold the Iraqis a few Stonefish already. If so, it seems unlikely to me that they'll work properly without reprogramming for the target signatures of US and UK shipping.

Incidentally, the classification >'UK restricted: commercial in confidence'< is among the lowest available. Almost all documents used by the armed services, including such things as reminder cards carrying the NATO phonetic alphabet, are classified 'restricted'; the term 'commercial in confidence' is applied merely in the fond hope that it will be respected, since it has only commercial meaning. The >'Technical Description and Specification' of Stonefish< may well be no more than the sort of thing small boys (like me) fill their carrier bags with every other year at Farnborough - I have collected stuff in the past on classified systems like JP233, also deployed in the Gulf. What these documents do not disclose is the true performance of the system and its strengths and weaknesses. That sort of information, operationally significant, is usually classified at a higher level (within NATO probably 'Secret').

Chaz

[All disclaimers apply.]

Flight simulator certification

<henry@zoo.toronto.edu> Tue, 4 Sep 90 13:16:21 EDT

<> Does anyone know the certification requirements for simulators?) >... I suspect there is nothing to cover >simulators, since they are not directly involved in controlling flight.

There *are* certification requirements for simulators when they are involved in pilot training, and in particular when used as substitutes for certain types of in-flight training. However, I think the emphasis has been more on precision than on accuracy, i.e. on the sophistication and smoothness of the simulation

more than on its exact correspondence to reality. Much is made, for example, of the quality of the visual imagery provided. I'm not sure how much has been done on verifying faithful (as opposed to merely plausible) simulation of behavior in obscure corners of the system.

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

✓ Glass cockpits

Martyn Thomas <mct@praxis.co.uk> Mon, 3 Sep 90 15:49:50 BST

The UK has a "confidential human factors incident reporting programme", run by the RAF Institute of Aviation Medicine, to allow aircrew to report incidents which may reflect badly on their competence, so that others may learn from them without any risk of the crewmember who made the report suffering any penalty. They have a magazine - FEEDBACK - and the last issue publicised the failure of most of the automated systems on an approach to a UK airport in a storm last February. (Reported in RISKS, I believe).

This issue carries a questionnaire asking flight crew for their opinions of automation. 78 questions of the form (ring the appropriate number)

"if the automatics fail it 1 2 3 4 5 if the automatics fail it is always apparent is never apparent "

The results of the survey will be *very* interesting. The survey is being carried out on behalf of the UK Civil Aviation Authority. It is not clear whether the results will be made public.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

"wild failure modes" in analog systems

Kent Paul Dolan <xanthian@zorch.sf-bay.org> Sun, 2 Sep 90 18:59:45 GMT

>From: Pete Mellor <pm@cs.city.ac.uk>

>Synopsis of: Forester, T., & Morrison, P. Computer Unreliability and >Social Vulnerability, Futures, June 1990, pages 462-474.

>In contrast [to digital computers], although analogue devices >have infinitely many states, most of their behaviour is >*continuous*, so that there are few situations in which they >will jump from working perfectly to failing totally.

Unless my understanding from readings in Chaos Theory is entirely flawed, the second sentence is simply false; it is now well known that analogue devices can also (through design infelicities or just the perverseness of the universe) do

inherently "wild" state switches. The classic example is the simple dribble of water from a faucet, which, in the absence of analogue catastrophes, would be a steady stream, or an equally spaced series of droplets, but is instead a series of droplets whose size and spacing is unpredictable except statistically.

More important, this is now understood to be the _usual_ state of affairs, not the anomalous one, in dealing with realistic analogue systems.

So, if the original authors' intent in demeaning our increasing reliance on (possibly "un-failure-proofable") digital systems is to promote a return to the halcyon days of analogue controls, this is probably misdirected by the time the controls approach the order of complexity of operation of the current digital ones.

We may just have to continue to live with the fact, true throughout recorded history, that our artifacts are sometimes flawed and cause us to die in novel and unexpected ways, and that we can only do our human best to minimize the problems.

Just an observation in passing.

Kent <xanthian@Zorch.SF-Bay.ORG> <xanthian@well.sf.ca.us>

🗡 Faultless Software

Robert L. Smith <rlsmith@mcnc.org> Tue, 4 Sep 90 13:25:43 -0400

The recent discussion in RISKS of the need for "ultrareliable" -i.e., faultless -- software and the impossibility of obtaining it has been interesting, but lack of it is no compelling reason to prohibit computers from life-critical service.

Advocates of that conclusion forget the reliability advantage software has over hardware and people system components, which is that once a software bug is truly fixed, it stays fixed! In contrast consider the many times you repair hardware only to see it fail again from the same cause, and coach people to do it right only to hear they've forgotten later.

Legal restrictions on software applicability would delay quality improvements. They would inhibit progress toward systems that truly are safer than those whose logic elements reside solely in human brains. Software in life critical environments is like old age: to understand its desirability, one has only to consider the alternative.

The question is, have more people died in life critical environments since software was installed than before, per man-hour of use? If the answer is no, then the argument is specious. Even if it is yes, which I doubt, that is reason only to intensify testing and debug. Software engineering has not yet built all the tools conceivable to that end.

Regards, rLs

✓ Comment on Software Reliability Synopsis

"Martin Minow, ML3-5/U26 03-Sep-1990 2253" <minow@bolt.enet.dec.com> Mon, 3 Sep 90 20:27:01 PDT

Thanks to Pete Mellor for posting >Synopsis of: Forester, T., & Morrison, P. Computer Unreliability and >Social Vulnerability, Futures, June 1990, pages 462-474. > Conclusion (quoted): >Accordingly, we recommend that computers should not be entrusted with >life-critical applications now, and should be only if reliability improves >dramatically in the future.

There is a risk/benefit that needs to be examined. If we remove computers from, say, hospital intensive care units because they are "unreliable" will we save lives that might be killed by an errant computer or kill others whose lives might have been saved by that same unreliable system.

>Given the evidence presented here, several ethical issues also emerge for
 >people in the computer industry. For example, when programmers and software
 >engineers are asked to build systems which have life-critical applications,
 >should they be more honest about the dangers and limitations?

Does the article really claim that engineers who know they are building life-critical applications are not honest about the dangers and limitations? My experience has been that people are quite aware of their responsibilites. On the other hand, systems that were never designed to be life-critical are often used in unexpected ways. Consider a speech synthesizer designed as a speech aid for a disabled person. While not designed as a "life-critical" system, it IS the voice that that person must use to call for help. What is an ethical professional to do? Refuse to build a speech synthesizer as it *might* be used in a life-critical situation and the technology doesn't yet allow us to design a perfect synthesizer?

>Are computer

>professionals under an obligation if a system fails: for example, if a patient>dies on an operating table because of faulty software, is the programmer guilty>of manslaughter, or malpractice, or neither?

Who cares? Will charging programmers with manslaughter really yield better quality software? This seems like exactly the wrong thing to worry about.

>How is it that the computer industry >almost alone is able to sell products which cannot be guaranteed against >failure?

Because people buy the stuff. Some software, by the way, *is* warrented against failure. All the type of warranty does is affect the price and time to market. I rather doubt that it effects the actual quality.

Martin Minow minow@bolt.enet.dec.com

✓ Database searches and counseling center confidentiality

&erek.Beatty@COSMOS.VLSI.CS.CMU.EDU> Tue, 04 Sep 90 12:23:42 EDT

Here's a minor variation on an old theme:

The Carnegie Mellon's online library catalog includes a full-text database of the faculty/staff directory, and can be used to look up anyone at CMU given their telephone extension. This brings to light a problem with confidentiality and the university's counseling center. If the counseling center phones a student and must leave a message, they leave only their telephone number and receptionist's first name, to protect against any stigma that might be associated with seeking their services. Easy access to the reverse telephone index function via database searching erodes this effort at confidentiality even though the library database publicizes no new information (it's all in the published hard copy directory).

Here again a large quantitative change (in lookup time) introduces qualitative differences (it becomes plausible that a roommate might snoop out of idle curiosity). Awareness of this might lead someone, feeling lowly as a (internet?) worm, to forego psychological services.

-- Derek Beatty, grad student, CMU Computer Science



Search RISKS using swish-e

Report problems with the web pages to the maintainer



March 1989 British Rail Train Crash

Brian Randell &rian.Randell@newcastle.ac.uk> Wed, 5 Sep 90 13:50:34 BST

[Yesterday's Independent carried a number of articles related to the ending of the trial of a British Rail train train driver in connection with a major train accident that occurred on 4 March 1989 in south London. There was a fairly lengthy front page article, and two further articles taking up a complete half-page. I have selected from these some paragraphs which should be on interest to RISKs readers. Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK PHONE = +44 91 222 7923 [Further excerpted by PGN]

A train driver who admitted passing through a red light and causing the Purley

rail crash, in which five people died and 87 were injured, was jailed yesterday. Robert Morgan 47, was sentenced to 18 months' imprisonment, 12 months of which was suspended, after pleading guilty to two charges of manslaughter. The sentence drew strong criticisms from the rail unions. The Old Bailey was told Morgan received two commendations in a previously exemplary 23 years as a train driver. [...]

Julian Bevan, for the prosecution, told the Old Bailey that Morgan was in hospital with face and neck injuries a few hours after the crash when he said he had jumped the red light at about 70mph. The track limit was 90mph. Describing the safety system thrown into question by the crash, Mr Bevan said drivers were given two amber warning signals before coming to a red light. Each is accompanied by a klaxon sounding in the cab. If the driver fails to switch it off, the brakes are applied automatically within three seconds, he told the court. Morgan, a single man, of Ferring, West Sussex, admitted that he must have switched off the klaxon each time, but the memory loss he suffered prevented him from being more precise. [...] Robert Morgan, a driver since 1966, had been well warned by the signalling system that there was going to be a train ahead of him. What went wrong?

For every signal a driver passes, the system provides him with an instantly recognisable set of acknowledgements. Every time a signal is passed at green, a bell rings in the cab indicating the line ahead is clear. If the signal is at double amber, or amber, or red, a klaxon sounds and has to be acknowledged by the driver. He has three seconds to do this and if he does not press the button, the brakes start to apply and are fully operational in five seconds. However, he can override this system.

It is a weakness in the system that BR has now recognised. The Purley crash came just three months after the disaster at Clapham where 35 people were killed when a signal failure resulted in a commuter express ramming another stationary rush hour train. The real cause, the public inquiry said, was too much repetitive, painstaking work, not enough time off - lack of supervision and improper testing procedures among technicians completing resignalling work in the area.

Since Purley, and acting on the recommendations of the Hidden Report into the Clapham disaster, BR has been overhauling its approach to safety.

BR admits that prior to the Clapham crash its approach to safety was equipment-based. It reasoned that if the equipment and the rules designed to protect it worked, then the safety of staff and passengers was assured. What happened at Clapham and to Robert Morgan at Purley showed that approach to be inadequate. In coming to terms with human error, BR has introduced its new Safety Management Programme.

Potential train drivers already undergo extensive psychological as well as practical testing, to ensure they are suited to working in a highly disciplined atmosphere. However, after work with Professor James Reason of the University of Manchester, a specialist in risk analysis, BR recognises that regardless of personality, all human behaviour is inherently quirky in increasingly repetitive circumstances. It understands that drivers can get into a "mind set" where they believe they have completed a task, or recognised a signal, when they have not. In that mental state, a driver could cancel a warning horn, not realise he had done so and plough on to disaster.

BR has admitted that the chances of an equipment failure being the sole cause of an accident have been all but engineered out of the safety equation, and that one of the biggest risks to passengers is drivers passing signals at danger. It happens on average between 20 and 30 times a year, and each incident is investigated. [...]

Complexity, safety and computers

Martyn Thomas <mct@praxis.co.uk> Wed, 5 Sep 90 10:57:39 BST

In RISKS (10.29), David Gillespie writes:

: I think one point that a lot of people have been glossing over is that in a

: very real sense, computers themselves are *not* the danger in large,

: safety-critical systems. The danger is in the complexity of the system itself

I agree. Often, people talk about "the software reliability problem" when actually the problem is the difficulty of getting complex designs right, and the impossibility of guaranteeing that any residual errors will cause the design to fail less frequently than (some very low probability of failure).

There is, of course, the related problem of what we mean by "getting the design right" and "failure". In general, these can only be defined with hindsight - we recognise that the system has entered a state which we wish it hadn't, and we define that as failure. We cannot (usually) guarantee that we have defined all safe states, or all hazardous states, in advance.

This is seen as a "software problem" because we *choose* to put most of the system complexity into the software, as a sensible design decision.

Recently, I have started to wonder if some of our difficulties are exacerbated by this decision. Software is digital (at the moment, at least). Yet many safety-critical systems involve monitoring analog signals and driving actuators which cause analog activity in the controlled system (for example, monitoring airspeed and driving the elevators of an aircraft). At some point in the system, the analog signal is digitised - generally before any computation is performed on it. Then the digital outputs are reconverted to analog.

The question I would ask is: are we making our systems significantly more complex by converting to digital too soon (or at all)? Would the system complexity be reduced if, instead of converting to digital so that we can use a commercial microprocessor, we processed the signals as analog signals, using an application-specific integrated circuit (ASIC) and only converted to digital where there is a clear reduction in complexity from doing so?

This is a serious question: latest technology allows mixed analog-digital ASICs, and the cost and time to produce an ASIC is competitive with the cost and time to produce the software and circuit board for a microprocessor system - and the technology is moving so that economics

increasingly favour the use of ASICs. You can have (some of) your favourite microprocessors on-chip, too.

To summarise: the issue is system complexity - safety is related (probably exponentially) to the inverse of complexity (if only we could measure it) - so reducing complexity is the key to increasing safety; can we make progress by exploiting analog techniques?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

software bugs "stay fixed"?

Martyn Thomas <mct@praxis.co.uk> Wed, 5 Sep 90 13:44:05 +0100

In <u>RISKS 10.30</u>, Robert L. Smith writes:

"... the reliability advantage software has over hardware and people system components, which is that once a software bug is truly fixed, it stays fixed! In contrast consider the many times you repair hardware only to see it fail again from the same cause ..."

I don't know how you define "truly fixed" (unless it means that the bug doesn't recur - in which case the claim that it stays fixed is tautological!).

In my experience, software bugs are often reintroduced (which is why regression testing is important). This source of problems is probably only surpassed by the number of *new* errors introduced while fixing old ones.

The problem of re-assuring software after "maintenance" is as hard as the problem of assuring it in the first place - while the industry practices are probably worse, and the regulatory control is certainly worse. Experience with "software rot" in past systems suggests that we may well see accidents caused by "faulty maintenance" in growing numbers over the next few years. I predict that the individual staff will be blamed, rather than the whole regulatory structure (whereas a major accident caused by an ab initio design error would raise the question of how the error managed to get through the certification process). Somehow, "maintenance errors" sound less threatening, possibly because they sound as though they only apply to a single system.

🗡 Re: Stonefish mine

<tmal@computer-lab.cambridge.ac.uk> Wed, 5 Sep 90 12:19:30 +0100

In <u>RISKS DIGEST 10.30</u> Chaz Heritage wrote in reply to a message from Pete Mellor:

>> 4. Does Stonefish rely on some sort of sonar transponder

>> to distinguish friend from foe?

>

> I imagine not, since if the mine were to transmit sonar in order to trigger
 > transponders located on friendly ships then it would render the mine very
 > susceptible to detection and countermeasures.

I don't know whether Stonefish is able to trigger transponders on detected ships but let us assume that it can. We already know that Stonefish performs pattern recognition on passing ships to distinguish friend from foe. There are also some types of hostile ships that should not be attacked, for instance we would like the mine to remain undetected as a minesweeper passes.

If the mine has already decided that a ship should not be attacked, because it has been deemed friendly or a hostile minesweeper, then it need not trigger the transponder. Only if it has already decided to attack a ship would it need to confirm its decision and so try to trigger the transponder. If there is no response then the mine intends to explode and so will almost certainly be detected very shortly afterwards.

The decrease in risk to friendly shipping may make such behaviour worthwhile; the additional warning that a foe would receive would be of the order of the round-trip time for the message pair.

Mark Lomas (tmal@cl.cam.ac.uk)

Ke: Stonefish mine

bill davidsen <davidsen@crdos1.crd.ge.com> Wed, 5 Sep 90 10:51:03 EDT

| From: chaz heritage:wgc1:RX| Date: 3-September-90 (Monday) 4:34:36 PDT

| > 6. The sophistication of Stonefish's recognition system argues for some | kind

of artificial intelligence. If it's that smart, would it know who was winning and change sides accordingly?<

| Personally I wouldn't consider Stonefish to be an AI. I don't think the | problem posed is much of a risk to Stonefish operators....

If, on the other hand, Carlos Cardoen is telling fibs (which would not
perhaps be entirely out of character) then it's possible that he's sold the
Iraqis a few Stonefish already. If so, it seems unlikely to me that they'll
work properly without reprogramming for the target signatures of US and UK
shipping.

Here's a real risk of software... after the mines are reprogrammed how would you like to be the first one to run a ship over one to verify that they are ignoring "friendlies?" Since Iraq doesn't have enough ships to worry about this, they don't have the problem, but if they blew the bottom out of a tanker they might really shut off the flow of oil.

I believe the mines huddle on the bottom and wait until they detect a target close enough to be damaged then pop to the surface. Somewhat like a "Bouncing Betty" mine, for those of us old enough to remember.

bill davidsen (davidsen@crdos1.crd.GE.COM -or- uunet!crdgw1!crdos1!davidsen) VMS is a text-only adventure game. If you win you can use unix.

✓ S-W controlled mine Risks to Aircraft carriers (Re: Stonefish)

William Ricker <wdr@wang.com> Wed, 5 Sep 90 18:06:16 GMT

I enjoyed the speculation "From Channel 4 news last night (Tue. 28th Aug)" about a software-controlled mine. However, after recent discussions in the sci.military / military-request@att.att.com list/group (initiated after I repeated something I heard a US Admiral say on CBC repeated over US NPR), I must quickly comment on:

In comp.risks, p.mellor@uk.ac.city (JANET) writes >It is reported that Iraq may be deploying some of the Royal Navy's latest >high-tech weaponry. Apparently this is causing US commanders to be reluctant >to send aircraft carriers into the northern area of the Gulf.

Carriers are not in the gulf because it it too small to maintain normal flight operations in -- the standard exclusion zones around a carrier task group would include oil platforms, Saudi, and Iran; and if operating in north gulf, Iraq. They also can't steam east or west for wind-accross-deck very long either, but that is less of a concern.

Stonefish may deter smaller ships and the Battleships (the forgotten class of capital ship) from approaching for bombardment, but they're irrelevant in that overgrown estuary for carriers.

/bill ricker/ wdr@wang.com a/k/a wricker@northeastern.edu

Reply to "Computer Unreliability" Stars vs Selves

Dave Davis <davis@mwunix.mitre.org> Wed, 05 Sep 90 11:04:23 EDT

In response to Peter Mellor's challenge in <u>RISKS 10.28</u>, 31 Aug 90, let me offer the following. On the surface, it would seem that the authors of the _Futures_ article have a fresh point of view about the risks of using computers in areas where the cost of failure is high, avionics, automated medical devices, nuclear reactors, etc. Systems based on large quantities of software do have large numbers of states, and therefore, large numbers of failure points. I addition, such a system may have previously unknown (to the developers) states caused by errors or outside factors, such as the EMI-caused failures of the Blackhawk helicopters. However, the arguments the authors present (as summarized by Mr. Mellor) are somewhat similar to previous objections to utilizing relatively immature technologies. That is, "we don't understatnd it well enough, so let's not trust it" is the underlying point. Almost any significant new technology fits that argument. Historically, it has been through applying a technology that motivation toward better theoretical understanding is created. For example, we didn't understand thermodynamics and statistical mechanics while we applied steam power for several generations. In addition, it is significant that the authors object to the use of statistics as a measurment technique. One wonders if this is an attempt to play on the commonly held bias against the use of statistics. Statistics are routinely used by all large manufacturing companies to identify production problems.

In broader sense, the authors misunderstand how broad the implementation of an information-intensive system can be. It is not necessarily just silicon and software. One is reminded of the complexity of the mechanical rail switching systems described so well in previous RISKS. The argument that discrete-state machines have inherently wilder failure modes that an analog systems isn't so. Any system that has feedback, intentional or unintentional, may behave wildly if a component fails, or it is operated outside design limits. (In the early 70s some airliners were thought to have crashed due to the pilots over-extending their controls.) Moreover, returning to the era of electromechanical devices that wear out and have their own idiosyncracies is not a path toward increased reliability.

Dave Davis, MITRE Corporation, McLean, VA

"Wild Failure Modes" in Analog Systems

Jim Hoover <hoover@cs.ualberta.ca> Tue, 4 Sep 90 21:45:06 MDT

Hmm, last time I taught a hardware course I emphasized that the digital computer was just a fiction invented by us theory types. All the implementations I know of use analog devices. Thus we already comply with the suggested legislation.

Jim Hoover, Dept. of Computing Science, University of Alberta, Edmonton, Canada T6G 2H1 | 403 492 5401 | FAX 403 492 1071 | hoover@cs.ualberta.ca

Re: Wild failure modes in analog systems

"Richard D. Dean" <rd0k+@andrew.cmu.edu> Wed, 5 Sep 90 11:23:01 -0400 (EDT)

>From: Pete Mellor <pm@cs.city.ac.uk>

>Synopsis of: Forester, T., & Morrison, P. Computer Unreliability and

>Social Vulnerability, Futures, June 1990, pages 462-474.

>In contrast [to digital computers], although analogue devices >have infinitely many states, most of their behaviour is >*continuous*, so that there are few situations in which they >will jump from working perfectly to failing totally.

Although analog behavior is continuous, what about resonance? While the output may still be a continuous function of some inputs, it's certainly very non-linear in some places....Watch the voltage (or current) on an RLC circuit go very high given the right (or wrong) frequency.

Drew Dean rd0k+@andrew.cmu.edu

Ke: "wild failure modes" in analog systems

Will Martin <wmartin@STL-06SIMA.ARMY.MIL> Wed, 5 Sep 90 14:49:04 CDT

>it is now well known that analogue devices can
>also (through design infelicities or just the perverseness of the universe) do
>inherently "wild" state switches. The classic example is the simple dribble of
>water from a faucet, which, in the absence of analogue catastrophes, would be a
>steady stream, or an equally spaced series of droplets, but is instead a series
>of droplets whose size and spacing is unpredictable except statistically.

While this is indeed true, I think that you have to look at the "level" of the possible state change to see the analog/digital difference. In the example cited, while each individual droplet is of unpredictable size and falls at (generally) unpredictable intervals, stepping back from the action and looking at the entire system (water pouring from the faucet) gives a predictable result -- over a period of time, a certain amount of water will flow out of that faucet.

There is not likely to be any sudden change in the rate of flow, nor is the flow likely to suddenly stop (assuming nobody is messing with the controls and there are no foreign objects in the water supply to clog the outlet). So while the individual elements (droplets) of the flow follow chaotic paths, the flow, as a whole, follows a predictable route.

In a digital system without adequate limiting controls, each succeeding digital number could vary wildly from the preceeding one. A high-order bit could be turned on, for example, causing an effect that just could not happen in an analog system, simply because it takes time for a change to occur; analog variables can "ramp" up or down but each instance will depend, to some extent, on those preceeding. Each digital sample, though, can stand alone and enormous swings can occur in the interval of milliseconds or nanoseconds between samples. Thus the possible range of catastrophic effects are inherently greater in digital as opposed to analog systems. (Of course, well-designed digital systems with limit checking and sample verification can avoid such ill effects.)

This doesn't mean that analog systems can't suffer similar catastrophes. In the example given, a lump of something in the water supply could clog the valve or nozzle in an instant. So the flow could drop to zero in a shorter-than-normal time. But that is about all that could go wrong. The flow couldn't change from 1 liter/minute to 1 billion liters/minute in an instant, or switch to a reverse-direction flow. A digital equivalent would be subject to such possibilities.

Will wmartin@st-louis-emh2.army.mil OR wmartin@stl-06sima.army.mil

// Re: "wild failure modes" in analog systems

Pete Mellor <pm@cs.city.ac.uk> Wed, 5 Sep 90 22:02:11 PDT

Kent Paul Dolan in <u>RISKS-10.30</u> writes about the "wild" (or "catastrophic" in Forester and Morrison's original terms) failure modes of analogue systems. He states:

> Unless my understanding from readings in Chaos Theory is entirely flawed, the >second sentence is simply false; it is now well known that analogue devices can >also (through design infelicities or just the perverseness of the universe) do >inherently "wild" state switches.

The "second sentence" here is:

<>In contrast [to digital computers], although analogue devices <>have infinitely many states, most of their behaviour is <>*continuous*, so that there are few situations in which they <>will jump from working perfectly to failing totally.

First, let me say that I *almost* entirely agree with Kent. After all, chaotic phenomena were originally demonstrated on analogue systems. In that synopsis, I was trying to present the authors' view without prejudice. I did not pick that particular bone with them in my subsequent criticism of their paper since I had plenty of other points to raise.

Kent goes on to say:

> So, if the original authors' intent in demeaning our increasing
> reliance on (possibly "un-failure-proofable") digital systems is
> to promote a return to the halcyon days of analogue controls,
> this is probably misdirected by the time the controls approach
> the order of complexity of operation of the current digital ones.

I agree again, *but*, we would never attempt to build systems of the complexity of our current digital systems if we had only analogue engineering to rely on. It would not be possible. Reliability requires simplicity. Analogue systems would be expected to be more reliable than digital because they are forced to be simpler. It is the complexity of the software in a digital system which leads to its unreliability. > We may just have to continue to live with the fact, true throughout
> recorded history, that our artifacts are sometimes flawed and cause
> us to die in novel and unexpected ways, and that we can only do our
> human best to minimize the problems.

Of course! No human endeavour is free of risk. However we do have a choice: a) to restrict the complexity of life-critical systems, in the hope of retaining some kind of intellectual mastery of their modes of failure, and b) to stop kidding ourselves that software failure makes an insignificant contribution to the unreliability of digital systems (and we *do* - see below [1]).

Returning to chaos (as properly defined: non-linear behaviour of a system, whose basic laws are well-understood, such that second-order effects predominate and the future states of the system become unpredictable at the detailed level since arbitrarily close points in the state space can diverge along widely differing circuits): how does this differ from digital system behaviour?

When Christopher Zeeman gave a lecture on Chaos at City, I asked him what he thought was the relevance of chaos theory to digital systems. To my surprise, he (and, I would guess, 99.99 per cent of other chaotists) had never given the problem a single thought! Hardly surprising, if you think about it. There *is* no physical theory of digital behaviour, and no distinction between 1st and 2nd order effects (or, if you like, everything is at least 2nd order: the slightest perturbation from a point in the state space can lead to *anywhere* arbitrarily quickly).

Has anyone out there thought about what the state space diagram of a modest digital device would look like? The closest I could get was a billion-dimensional discontinuous space of 0's and 1's (i.e. the Cartesian product, a billion times over, of {0, 1} with itself). Yuk!

A serious attempt *has* been made (by John Knight - reference not to hand) to examine the shapes of bugs in programs, i.e. the topological properties of those subsets of the input space which activate program faults. Chaotists will be pleased to learn that they were fractal.

So here I side with Forester and Morrison. Although I agree with Kent that analogue systems can behave chaotically, digital systems are far, far more chaotic than chaos!

Just an observation in passing.

[1] By the way, the reference above to belief in the perfection of software is based on what a representative of Airbus Industrie said when interviewed on the last Equinox programme on fly-by-wire (see RISKS passim).

UK viewers (and some elsewhere in Europe) should tune into Channel 4 on Sunday 30th September, when an updated version of this programme will be transmitted. Approximately 50 per cent of the material is new, including some *very* interesting stuff on the Mulhouse-Habsheim disaster.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)





Robert E. Van Cleef <vancleef@prandtl.nas.nasa.gov> Thu, 6 Sep 90 07:34:41 -0700

In the Business section of the 9/5/90 San Jose Mercury News, Page E-1, the column "Bits & Bytes", by Rory J. O'Connor and Valerie Rice, discusses an new class of "Trojan Horse" for PostScript printers.

According to the article, there is a "clip art" file, written in PostScript, that "surreptitiously reprograms a chip inside the printers, changing a seldom-used password stored there. When the password is altered, ... the printer no longer functions properly."

A Minneapolis company, Multi-Ad Services is listed as claiming to have a free "vaccine".

Bob Van Cleef - vancleef@nas.nasa.gov, RNS Distributed Systems Team Leader

Floating Point Emulation required for Ultrix systems

Dave Wortman <dw@csri.toronto.edu> Thu, 6 Sep 90 15:43:57 EDT

I had a very bad experience in trying to configure an Ultrix system that may be of interest to comp.risk readers.

Most Unix systems are generated from a "configuration file" which selects optional software to be included in the Unix kernel. A system utility (/etc/config) processes the configuration file to build a directory of components for the Unix kernel. These components are then compiled/linked together to build a Unix kernel.

In the early (PDP-11) days of Unix, a package for performing emulation of floating point arithmetic was included in the Unix kernel because the underlying hardware didn't support floating point arithmetic. One of the options that can still get included in a configuration file is:

EMULFLT Emulates the floating point instruction set if it is not already present in the hardware

I was browsing through the configuration file for a DEC Ultrix system and decided in a fit of excessive tidiness to delete the EMULFLT option. After all the machine had this expensive floating point hardware and I would probably gain both space and performance in the kernel. The configuration tool built a system directory without complaint and I was able to compile and link a new Unix kernel without any error messages.

The trouble began when I tried to boot the new Unix kernel (on a DEC 3600). One of the first programs that gets run once the kernel has been initialized is a system utility (/etc/fsck) which validates the root filesystem by checking all nodes and links for reasonableness. Under the new kernel /etc/fsck failed with an undocumented error message and an indication that the root file system was corrupted. Since this check is deemed to be vital to the correct operation of Unix, the entire boot process aborted. Booting an old version of the kernel worked correctly and failed to discover any problems with the root filesystem.

This was NOT an easy problem to diagnose.

It took a long time and a lot of painful head scratching to discover that the fsck utility (or some routine that it called) depended in some subtle way on software that was included by the EMUFLT option (on a 3600 it may have been some complicated string instruction rather than a real floating point operation). Once I restored floating point emulation to this 4th generation machine, the system began behaving normally again. There are several RISK-related lessons to be learned from this experience:

- one shouldn't casually muck-about with system parameters unless one is willing to spend the effort to learn how to adjust them properly.
- it is bad system design to document a parameter as an "option" when in fact it is mandatory for the correct operation of the system. Until dependencies on floating point emulation are brought under control, the user probably shouldn't have the option of building a system without EMUFLT and the configuration tool should enforce this restriction.
- EMUFLT appears to be misnamed and misdocumented as well, it probably causes the inclusion of software other than just floating point emulation.
- it is bad system design for a utility program to depend on an optional component of its environment without verifying that the optional component is available. /etc/fsck should have checked for the presence of floating point emulation and displayed an appropriate error message if it was unable to continue.

Ke: Software bugs "stay fixed"? (<u>RISKS-10.31</u>)

Dave Parnas <parnas@qucis.queensu.ca> Wed, 5 Sep 90 20:02:15 EDT

My perception is that they stay fixed, if they were actually fixed. Usually they were not properly corrected and, under new circumstances, problems reappear. Then it appears as if the bug recurred. Actually, it had never gone away.

re: Wild failure modes and COMPLEXITY

Rochelle Grober <rocky@argosy.UUCP> Thu, 6 Sep 90 14:07:27 PDT

With regards to wild failure modes of digital versus "continuous performance" of analog devices, this seems to me a pure fallacy. Analog devices can display as great and rapid a change to the system as digital devices.

One of the most graphic historical instances of this is the blackout of New York City in the '60's. The blackout, which threw New York into a night of turmoil, and affected a large portion of the city, was do to one relatively small power generator in the Chicago area failing "open", what was considered a benign type of failure. Unfortunately, New York was connected to the same power grid, and was a quarter wavelength away. The distance is extremely significant, as the power stations in New York received the failure as a "short". Massive amounts of power surged through the New York power stations and destroyed the safeguards along with many of the systems. Until this event, no one ever considered it to be a possibility. No computers involved, small error action, huge error reaction of an analog system.

This is an example of why much of industry has gone to digital controls. Yes, they are complex, but they have discrete, limited numbers of responses. Modelling simple analog systems is much more complex than modelling a digital system of similar complexity. Periodic functions such as those involved in fluid dynamics (air, electricity, liquids, quantum mechanics, etc) require analysis in not just time, but frequency domain as well. Maxwell's equations are generally not necessary in simulating digital designs, but must be accounted for in every analog electrical system.

The real issue is complexity, as has been stated by others. Every technology which pushes the limits of the implementor's understanding contains the prospect of unpredicted behaviour. Digital controls simply have pushed the limits farther, by allowing the less complex (sometimes read as fewer states) discrete technologies to succeed the problematic, continuous state analog technologies.

--Rochelle Grober

Re: Lawsuit over specification error

Brinton Cooper <abc@BRL.MIL> Tue, 4 Sep 90 23:59:13 EDT

Pete Mellor and Martyn Thomas agree that

<> You cannot expect crew to do better than their <> training under the stress of an emergency.

Er...the crew are, after all, thinking humans and merely another set of automatons in the system. A recent (past 5 years) air crash in the mid-US was less disastrous than it might have been precisely because the pilot performed beyond his training, in a situation which he had not been expected to encounter. This is, after all, one of the differences between human and machine.

_Brint

Re: Flight simulator certification (<u>RISKS-10.30</u>)

Steven Philipson <stevenp@decwrl.dec.com> Tue, 4 Sep 90 18:41:17 PDT

In <u>RISKS DIGEST 10.30</u> henry@zoo.toronto.edu (Henry Spencer) writes:

>There *are* certification requirements for simulators when they are >involved in pilot training, [...] However, I think the emphasis has >been more on precision than on accuracy, i.e. on the sophistication >and smoothness of the simulation more than on its exact correspondence >to reality. [...]
The fidelity of simulators to their real-world counterparts is of paramount importance. It is intended that simulators mimic the performance of the actual aircraft as closely as possible, so that techniques learned in the simulator will actually be helpful in the aircraft. A tremendous amount of effort goes into confirming the fidelity of these systems.

High fidelity of simulation is difficult to obtain and maintain. Models of aircraft performance may not be perfect, but the errors may be difficult to detect. A small variation in simulator behavior has been suggested as a contributing factor in the crash of a DC-9. In this case, the simulator produced a visible yaw in the direction of a failed engine that wasn't present during an actual failure. It was theorized by the NTSB that the crew mis-identified the failed engine BECAUSE they expected the yaw shown in the simulator, and that this led to a loss-of-control accident.

Aircraft in the field are often modified, and changes are also made at the factory. Thus a given simulator may have at one time accurately reflected some number of airplanes, but may not be configured identically to any given airplane currently in use.

Full-scale simulators are intended to be so like the actual aircraft that one can be certified to fly the aircraft while only flying the simulator. In such cases, fidelity is more important than reliability -- if the simulator is working, it should mimic the performance of the aircraft perfectly. An unreliable simulator would be more acceptable than one with low fidelity, i.e. it much more acceptable for a simulator to shutdown and have to be restarted once an hour than it would for it to run continuously but incorrectly mimic the performance of the aircraft.

It should be noted that perfect behavior by a simulator is not always necessary for the simulator to be useful. Many low-cost simulators for light aircraft have some startling performance artifacts but continue to be effective training aids. For example, when the Pacer Mark II simulator is rolled inverted, "up elevator" still produces a climb. This is obviously wrong performance, but it is outside the stated limits of the simulator performance (bank angle limits are less than 90 degrees). This particular device has other interesting artifacts, but it still is useful for certain types of training activities. In recognition of its limitations, it is formally referred to as a "ground procedures trainer", but its function is to simulate certain modes of flight.

There is a tradeoff here, just as there is with other technological systems. Imperfect behavior of simulators may contribute to accidents, but by and large, their use helps to prevent many more.

Steve Philipson

Ke: Lawsuit over simulator specifications (<u>RISKS 10.27</u>)

Robert Dorsett <rdd@ccwf.cc.utexas.edu> Tue, 4 Sep 90 19:53:07 -0500

Martyn Thomas <mct@praxis.co.uk> wrote:

>: This claim seems to me to suggest (a) that once again, aircrew do not

>: understand the side-effects (pitch-up, in this case) of flight-director

>: commands (which I believe means that the systems are too complex).

Oh, they understand it, all right--they're just encouraged to put a very high level of faith on it. It's no wonder that people might become fixated on the flight director, and neglect the rest of the scan. In fact, some airline procedures seem to encourage such a practice, these days.

When one flies a flight director, one is, in effect, flying the airplane like an autopilot would. This has the effect of putting the pilot in "the loop," but has the problem of having him hanging off the flight director system.

>: critical systems such as simulators - on this evidence, a simulator used for
>: crew training in emergency procedures is *itself* a safety-critical system.
>: (Presumably it should therefore require certification in the same way as an
>: in-flight system of equivalent criticality.

They are certified to a fairly hard standard. For more information, see Rolfe's _Flight Simulation_. He covers the certification, installation, and testing components of a simulator delivery. However, also pay attention to how much of flight simulation is dependent upon specific customer requirements (no need, for instance, for a motion system, if all the simulator is going to be used for is systems familiarization) and how much perceptual data is outright fudged. Flight simulation is an art, not a science. When one flies a simulator, one is flying a concept of how the airplane flies; one is not flying in a terribly rigorously defined mathematical model. Even though a simulator almost always, these days, uses actual airplane avionics, and is almost 100% component-identical to a real cockpit, the way the instruments WORK is always subject to refinement. In the specific case of Northwest vs. CAE, it is Northwest's responsibility to supervise the development of the simulator, and, upon delivery, test it to ensure that it met specifications. Everyone does it this way; I suspect that Northwest's legal department may have found a legal technicality to relieve them of their responsibility.

>Does anyone know the certification requirements for simulators?

Rolfe mentions the various certification authorities' requirements. In addition to these, FAR 121, Appendix H covers the training requirements.

Advisory Circular 120-45 and 120-46 (1987) cover the entire spectrum of Advanced Training Devices.

Advisory Circular 120-40A (1986) covers simulator and visual systems evaluation.

Note that all documents are subject to review, as reflected in the Federal Register; it often takes a couple of years for changes to be reflected in the "officially" published documents. Contact your local FAA office for more

info.

Incidentally, I think it's only a matter of time before some bereaved widow attempts to sue Microsoft, after hubby tries to land on top of the World Trade Center. :-)

Robert Dorsett UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

Computers and Safety

<HMurray@DOCKMASTER.NCSC.MIL> Wed, 5 Sep 90 21:49 EDT

>Synopsis of: Forester, T., & Morrison, P. Computer Unreliability and >Social Vulnerability, Futures, June 1990, pages 462-474.

>From the synopsis and criticism posted, I have concluded that this work is probably useless "computer bashing." On the other hand, the discussion that it has prompted has been both useful and fascinating.

For example:

In RISKS (10.29), David Gillespie writes:

>I think one point that a lot of people have been glossing over>is that in a very real sense, computers themselves are *not* the>danger in large, safety-critical systems. The danger is in the>complexity of the system itself.....

Nonetheless, the application of the computer adds a great deal of complexity that might not be there in its absence. It results, in part from the complexity of the computer itself, in part from its inherent generality, and in part, from the failure, resistance, or reluctance of the programmer to manage it down.

Much of the generality of the computer resulted from the perception that it had to be broad in application in order to get copies up and unit cost down. The early RISC research demonstrated that this may not be so, but so far we have been reluctant to employ simple architectures. For example, we have known about finite-state machines for a long time, but few have been successful in the market for any application, much less safety-critical applications.

Likewise, there has been great resistance on the part of programmers to give up demonstrably error-prone programming constructs, such as the infamous GOTO. (Even using it as an example is likely to start a new defense.) Generality and flexibility seem to be much more highly valued than simplicity. The result is gratuitous and unnecessary complexity heaped on the necessary. Martin Thomas makes an interesting and related observation:

>There is, of course, the related problem of what we mean by >"getting the design right" and "failure". In general, these can >only be defined with hindsight - we recognise that the system >has entered a state which we wish it hadn't, and we define that as >failure. We cannot (usually) guarantee that we have defined all >safe states, or all hazardous states, in advance.

But part of the problem is that there are an infinite number of states. A finite-state machine with a limited number of states would limit the potential for error.

Thomas continues:

>The question I would ask is: are we making our systems
>significantly more complex by converting to digital too soon
>(or at all)? Would the system complexity be reduced if, instead
>of converting to digital so that we can use a commercial
>microprocessor, we processed the signals as analog signals,
>using an application-specific integrated circuit (ASIC) and only
>converted to digital where there is a clear reduction in
>complexity from doing so?

There are two questions here, not one. The first has to do with the use of analog vs. digital. And the other has to do with "application specific." Each of these has the potential to reduce the complexity. Each should be applied where it is applicable.

>This is a serious question: latest technology allows mixed
 >analog-digital ASICs, and the cost and time to produce an ASIC
 >is competitive with the cost and time to produce the software and
 >circuit board for a microprocessor system - and the technology
 >is moving so that economics increasingly favour the use of ASICs.

Agreed, but then he continues further:

>YOU CAN HAVE (SOME OF) YOUR FAVOURITE MICROPROCESSORS ON-CHIP, >TOO.

You sure can, but the favoritism is part of the problem, not the solution.

>To summarise: the issue is system complexity - safety is >related (probably exponentially) to the inverse of complexity (if only we >could measure it) - SO REDUCING COMPLEXITY IS THE KEY TO >INCREASING SAFETY; can we make progress by exploiting analog >techniques?

Perhaps, but there is no question that we can reduce it by employing finite-state application-specific processors.

William Hugh Murray, 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL



Report problems with the web pages to the maintainer



"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Fri, 7 Sep 90 10:19:42 PDT

The herein-debated list of critical computer applications, in which reliance on computers is to be avoided includes, re defense, mere early warning systems. Presumably, Space Command's rate of false alerts, and the Vincennes shootdown, contribute to this opinion. But there is an important nuance neglected in challenging the warning systems -- early warning is clearly beneficial, problems arise only when an immediate ("use-or-lose") decision to retaliate is contingent upon it. Thus, it is really the de facto computerization of decision-to-shoot procedures that is at fault, not the neutral computerization of warning information.

And so I would not avoid early warning systems, which can greatly assist taking evasive or preparatory actions, but would squarely challenge the computerization of command and control systems. The leading example of such damnably dangerous computerization is the under-development, half-billion dollar Rapid Execution And Combat Targeting system, which will enable virtually instantaneous launch of U.S. ICBM's within a couple of minutes, at all times. This includes the introduction of PC's into launch silos, which will automate launch code verification, and which will provide some sort of direct electronic interface with the missiles.

Besides actualizing launch on warning and sudden first strike capabilities, the implementation of REACT would seem to add to the risk of an accidental launch, even without a flimsy attack warning. (If launch codes are received at the silos, standing orders require their immediate execution...)

Complexity, reliability, and meaningless arguments

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Thu, 06 Sep 90 19:50:38 -0700

To save my having to mail this information individually to the many people who have asked:

The next meeting of SC 167 (the RTCA committee rewriting DO-178A) will be November 6-9 in Herndon VA (outside of D.C.). You can get on the mailing list for notification of meetings by calling the RTCA (Radio Technical Commission for Avionics) at (202) 682-0266.

With regard to the complexity discussion, does the question of whether one generic type of system is more complex or more reliable than another even make any sense? The same function can be implemented in a simple or "complex" way using any generic type of components.

Consider Rube Goldberg's design for a "simplified" pencil sharpener. It starts with a string attached to a kite flying outside a window. When the window is opened, the string lifts the door on a cage filled with moths allowing them to escape and eat a red flannel shirt hanging above the cage. As the weight of the shirt decreases, a shoe (attached to the top of the shirt via a string through a pulley) becomes heavier than the shirt and starts to move downward, flipping a power switch on. When the power goes on, an iron on top of some pants on an ironing board burns a hole in the pants, creating smoke which enters a hole in a tree trunk next to the ironing board, smoking out an opossum which jumps into a basket from a higher hole in the tree, pulling a rope that lifts a cage door allowing a woodpecker to chew the wood from the pencil exposing the lead. There is also an emergency knife which is always handy in case the opossum or the woodpecker gets sick and can't work.

One could argue that Goldberg's simplified design has a larger number of failure modes with a high probability of occurring and therefore will be less reliable than more traditionally-designed pencil sharpeners. However, his design, although it may fail more often, has the backup knife which may result in a higher probability of resulting in having a way to get your pencil

sharpened (even if a cat comes in through the open window and distracts the opossum and the woodpecker) than a traditional pencil sharpener without the knife. So it is not only the number and probability of the failure modes that counts, but also the ways you have provided for coping with component failure.

Consider also that a knife alone would be much more reliable than even a regular pencil sharpener (especially one of the Ginzu knives that the TV spokespeople tell me never get dull). But it is definitely less safe in terms of potential for drawing blood. So if safety rather than reliability is your higher priority goal ...

When comparing the reliability and safety of mechanical/analog systems and digital systems, you need to consider:

- Confidence and the ability to measure or assess reliability and safety in our systems may be more important than other factors.
 I would prefer to design critical systems with components having known failure modes and failure rates than those that MIGHT have lower failure rates, but also might have higher ones and I have NO way to determine this with high confidence.
- 2) Analog and mechanical designs are often reused and perfected over long periods of time. Not only does this tend to eliminate design errors, but it allows for high confidence in the failure rates and the projected failure modes. Do unexpected failure modes pop up occasionally that were not expected? Sure, so what? -- the alternatives are worse.
- Wearout failures are much easier to detect and protect yourself against (e.g., simple redundancy usually provides adequate protection) than design errors resulting in erroneous answers.
- 4) Tools and methods for building systems reliably and safely may be as important as other factors. For example, system safety engineers have many time-honed procedures for assessing and enhancing safety in analog/mechanical systems but few of these have been extended to digital systems. Same applies to mechanical engineers. And they tend to be trained in using these procedures.
- 5) Because it is (seemingly) easy to provide a great deal of functionality with little increased cost or trouble, digital components tend to have greater functionality demanded of them (it is the usual argument for replacing mechanical/analog devices). This increases the probability of design errors.
- 6) ... [lots of other complicating factors]

Ke: "Wild Failure Modes" in Analog Systems (Hoover, <u>RISKS-10.31</u>)

<wolit@mhuxd.att.com> Fri, 7 Sep 90 10:02 EDT

Might as well carry this nit-picking one level further. As long as

your computer's transistors, capacitors, or whatever rely on electrons, photons, or other quantum-mechanical wave/particles with discrete states, you are justified in considering them to be digital. But this is all silly -- the implementation is irrelevant. If you can treat the computer as a black box that behaves digitally, why not label it as such?

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

Analog vs Digital Controls

Martin Ewing <WING@Venus.YCC.Yale.Edu> Thu, 6 Sep 90 22:27 EDT

Analog controls are not really the opposite of digital. The main difference is that digital logic often uses saturated transistors and obscure data coding as a representation, or analog, of a physical parameter. Digital systems do tend to use an enormous number of transistors for even the simplest operations, but they are integrated into a manageable number of chips.

Analog systems are plagued by poor gain calibrations, temperature drifts, nonlinearities, and noise. Nonlinearities can result in saturation and "latch-up" behavior. AC systems suffer from crosstalk, parasitic oscillations, and lots of other ills. A component failure can easily produce as drastic a change in output as a digital failure might.

The "advantage" of analog systems is that they don't have software. However, they do have all the troubles listed above, which tend to limit functionality. They also have circuit designers instead of programmers.

The safest control systems are passive ones, which use no analogs: reactors that get less reactive at high temperatures and aircraft that fly themselves with no control forces.

Martin Ewing, 203-432-4243, Ewing@Yale.Edu Yale University Science & Engineering Computing Facility

🗡 Chaos

Peter da Silva <peter@ficc.ferranti.com> Thu Sep 6 22:33:54 1990

> Thus the possible range of catastrophic effects are inherently greater in> digital as opposed to analog systems.

Like the Tacoma Narrows bridge?

Peter da Silva. +1 713 274 5180. peter@ferranti.com

Ke: Software bugs "stay fixed"? (<u>RISKS-10.31</u>, Parnas <u>RISKS-10.32</u>)

&ruce_Hamilton.OSBU_South@Xerox.com> Thu, 6 Sep 1990 19:09:43 PDT

Re: "My perception is that they stay fixed, if they were actually fixed."

A nontrivial portion of the bugs we encounter in building and testing our large systems are INTEGRATION (system-building) errors, where the wrong version of some software was included. Coding errors are only HALF the reason for regression testing.

Bruce BHamilton.osbuSouth@Xerox.COM 213/333-8075

Ke: Software bugs "stay fixed"? (Parnas, <u>RISKS-10.31</u>)

K. M. Sandberg <sandberg@ipla01.hac.com> 7 Sep 90 11:37:16 GMT

One problem is that sometimes the source code is not managed properly and code that has the bug is reintroduced when fixing another bug. Also it is possible that the code was "shared" and used in other programs/subroutines or the logic that caused the bug is still in the programmer's head. Major updates to the code could also lead to the reintroduction of the bug for several reasons including some one removing the fix as it seems not to be needed (lack of comments?)

In other words there are many things that could cause the bug to reappear when it was really fixed. This is the real world where anything is possible (Remember Murphy's Law).

Kemasa.

Ke: Software bugs "stay fixed"? (<u>RISKS-10.31</u>)

<ark@research.att.com> Fri, 7 Sep 90 09:29:12 EDT

I have had more experiences than I care to think about in which bugs have been fixed, and fixed correctly, but then somehow the wrong version of the program was sent to the user.

My `debugging rule number 0' is: before you go looking for a bug, make sure the program you're looking at is the one you're running. You'd be amazed how many bugs have disappeared that way.

--Andrew Koenig

Ke: Software bugs "stay fixed"? (Parnas, <u>RISKS-10.32</u>)

Michael tanner <mtanner@gmuvax2.gmu.edu>

Fri, 7 Sep 90 09:35:41 -0400

In practice the following occurs:

1. Programmer A fixes a bug. Some time later programmer B is given the same software to fix a different bug, or otherwise make changes. He sees some extraneous code he doesn't understand, doesn't see how it could work, or whatever and in an attempt to clean up the program, deletes or changes it. This turns out to be programmer A's bug fix, and the old bug is reintroduced.

Or,

2. Large systems get re-built occasionally, and sometimes with old versions of some routines, thus introducing old "fixed" bugs.

Users are accustomed to seeing old bugs resurface, and programmers often find the above scenarios to be the cause. Maybe good software practice would prevent it, but it does happen.

-- mike

Michael C. Tanner, Dept. of Computer Science, George Mason University

Moot camping (Ultrix, Wortman, <u>RISKS-10.32</u>)

Timothy VanFosson <timv@cadfx.ccad.uiowa.edu> Fri, 7 Sep 90 14:49:11 GMT

I too had a similar problem because of *my* fit of tidiness. Although my machine (a VS3100) would boot, certain login ids would would be required to go through the login process (Xprompter) two or three times before they would actually work. I know this is true because my id was one of them. I guess an added risk to the situation is that you may go crazy trying to remember your last three months' worth of passwords before you figure out that it is an OS problem :-).

Timothy VanFosson, Senior Systems Analyst, University of Iowa CAD-Research, 228 ERF, Iowa City, Iowa 52242 Phone : (319) 335-5728



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Sat, 8 Sep 1990 12:49:01 PDT

In August 1989 the town of Tisbury, Massachusetts, signed a \$113,000 contract for a computer system, but a town meeting in October nixed the deal. The vendor refused to take the system back, and sued the town. The town left the CPU and printer plugged in, because they were uncertain whether just pulling the plug would cause any damage, and because they did not know the "secret password". Finally, this August the vendor agreed that if the town would negotiate, they would divulge the password to the town consultant, Eric Ostrum, who could then shut down the system.

While the attorneys were negotiating, the consultant read the manual instructions, got the system to answer "Do you want to shut down the system?", and typed "yes". Then, the system shut itself down, with no password required! So he called the town's attorney and told him not to bother to negotiate for the vendor assistance. [Source: An article by Rachel Orr in the Vineyard Gazette, 28 August 1990.]

[MORAL: The next time you want to hot-dog a vendor, let Ostrum hire weenies.]

French prisoners use "smart cards"

Robert Nagler <nagler@olsen.UUCP> Sat, 8 Sep 90 18:41:10 +0200

Prison `a la carte", The Economist, 8 Sep 1990, p 33:

"Barely had the first miscreants arrived at France's newest prison, at Neuvic in the Dordogne, than they started a riot. Keen though the appetite of French prisoners is for insurrection, their protest did not result from force of habit. The inmates of the ultra-modern jail had taken unkindly to exactly the measures designed to make their lives more bearable.

"In particular they objected to being locked up by computers. Neuvic, which opened two months ago and is still filling up, is a technological strongbox containing the best ideas the penal service has so far come up with. Every prisoner carries a personalised ``smart card'', which must be used to enter or leave any part of the prison. The cards tell the central computer where all the prisoners are, [or at least where their cards are :-] all the time, and make the constant vigil of warders unnecessary.

"In other words, the prisoners inform the security system. It was hoped this might give them a satisfying sense of responsibility, but the signs are not promising. Inmates liken the jail to a computerised warehouse where they are stored as goods. For example, if a man is a minute late for breakfast, he cannot get out of his cell: the smart card works only to pre-programmed times. The convicts also complain of prices in the prison shop that are 20% higher than in other jails; cynics point out that Neuvic is being experimentally run by private enterprise." [After recently having been robbed in the south of France, I have absolutely no sympathy.--RJN]

[Excerpted by PGN, who thought it must have been a smarte garde.]

Instrument Software failure in BAe aircraft

<sean@aipna.edinburgh.ac.uk> Sat, 8 Sep 90 13:19:49 BST

>From The Guardian, September 8, 1990, page 2, column 7

Serious Failure' on BA planes (Patrick Donovan, Transport editor)

Instrument Panels on three British Airways aircraft `crashed' on eleven occasions shortly after take-off or landing because of computer software faults, according to Company Documents. The problems occured on short-haul European and domestic flights by three of the airline's British Aerospace Advanced Turbo Prop aircraft in a period between July 9 and August 20 last year. Special restrictions were imposed on the 64-seater aircraft by the Civil Aviation Authority because of the problems. BA was told that pilots must be in their seats when the aircraft flew below 5,000 feet in case emergency action was needed. Takeoff and landing was restricted to a minimum of 1,000 metres visibility, the documents say.

Two of the aircraft affected continued flying although they had experienced failure of `captain's and co-pilots primary displays' twice in one day. One of the aircraft, call sign G-BTPJ, suffered instrument failure five times on fights between Belfast, Manchester, Glasgow, Aberdeen, Bremen, Berlin and Manchester [sic]. Pilots were alerted by the caption `I/O Fail' flashing onto a blank screen. Aircrew managed to restore instrument readings after following emergency technical procedures, the papers say.

A BA spokeswoman said last night that the problems had been rectified. She said that safety was not compromised as backup systems were available despite loss of `primary instrument panels'. However, the BA document described the problems as being of a `serious nature'. According to the papers the `cause of the failures was due to a design shortfall' in instruments made by Smiths Industries. `Three incidents involved failure of all four displays which required the aircraft to be flown using the standby instruments until the displays were restored. All the failures reported occured during the initial climb, or climb phase with the exception of one incident which occured during the approach.'

The documents also explain how BA is developing a 'totally new code of practice for dealing with major accidents'. The report, circulated amoung BA operational staff, says: 'it is an inevitable fact of life that pilots, engineers, operational personnel, indeed everyone involved in the operation of aircraft will from time to time make professional errors. Some of these mistakes may result in an incident.'

Captain Colin Seaman, BA's head of safety, urges staff to be frank about accidents. 'No matter what temptation there is after an accident to be economical with the truth when rationalising it with hindsight, please remember it would be unforgivable if, by not revealing the facts or the complete truth, a similar incident became an unavoidable accident.'

[What a wonderful sentence! Reminds me of my favorite legal phrase, "Nothing in the foregoing to the contrary notwithstanding, ..." PGN]

MW's 'autopilot'

<SNYDER@csi.compuserve.com> 05 Sep 90 17:42:04 EDT In regard to BMW's "Heading Control System", my understanding (based solely on hearsay) is that the guidance system provides more of a gentle nudge than an irresistable shove when it thinks the car is approaching a lane divider line. Thus, it should not be difficult to leave the lane on purpose, either to pass or to get out of danger. However, has anyone thought of a more distressing problem? I refer you to countless "Roadrunner" cartoons. Picture a nice shiny white line leading directly into the side of a mountain...

Michael Snyder, Compuserve

// Re: "wild failure modes" in analog systems

<henry@zoo.toronto.edu> Fri, 7 Sep 90 14:27:22 EDT

>... we would never attempt to build systems of the complexity>of our current digital systems if we had only analogue engineering to rely on.

Unfortunately, this is not entirely true. Very complex analog systems were not at all unknown in pre-digital days. Concorde's engine computers are analog circuitry, which makes them a maintenance nightmare by modern standards -- each setting interacts with others, so readjusting them is a lengthy and difficult chore. (It is not worth developing a digital replacement for such a small number of aircraft.) For another example, I believe the US Navy's four ex-WWII battleships are still using their original *mechanical* analog fire-control computers. For still another, although the recent fuss about fly-by-wire systems for aircraft has focused mostly on digital versions, analog fly-by-wire systems were not at all unknown: Avro Canada's Arrow interceptor was flying at Mach 2 with analog fly-by-wire in 1958.

Certain jobs simply require complex systems, and will be done one way or another. It is probably true that digital implementations make it easier to add *unnecessary* complexity, but they also make it easier to do a better and (potentially) more foolproof job on the basics. This argument has many parallels to the old ones about whether word processors lead to poorer writing, or whether 16-bit address spaces forced better programming. Analog circuitry does encourage simplicity, yes... by making design, testing, and maintenance of even simple systems more difficult. This is not necessarily a virtue.

Henry Spencer at U of Toronto Zoology utzoo!henry

Re: Dealing with software complexity

"Martin Minow, ML3-5/U26 07-Sep-1990 1555" <minow@bolt.enet.dec.com> Fri, 7 Sep 90 13:12:24 PDT

Several Risks postings have discussed system complexity and whether "risks" are affected by, say, using analog components or finite-state automata.

One advantage to putting parts of the system into an analog component is that it separates the problem into isolated (and smaller) units that can be implemented and tested independently. The benefits of isolation might outweigh the disadvantages of analog designs. Of course, such a system could also be built out of all-digital components with a/d and d/a convertors at the final stages.

Much the same can be said for finite-state automata. Hand-encoded automata offer a good development methodology for many problems as it is simple to know when all state/action pairs are covered. On the other hand, finite-state automata generated by compilers (such as Unix' lex and yacc) can be fiendishly difficult to hand-check as the "intelligence" is distributed among a number of extremely obscure tables. (In passing, I would make the same complaint about object-oriented programming techniques.)

Martin Minow

[At least you were not CoOOPTed by a lex barker. PGN]

Ke: Software bugs "stay fixed"?

Robert L. Smith <rlsmith@mcnc.org> Fri, 7 Sep 90 21:17:40 -0400

Mr. Thomas implies that it is impossible to be certain, other than by nonrecurrence, that a nontrivial software bug is fixed. My experience indicates otherwise.

Just last week I was faced with misbehavior in a new program to analyze tablet input, where the analysis depended upon prior selection of an input sequence two or more PELs apart on either coordinate. But close examination revealed that points were occasionally being selected in adjacent PELs. This could occur because, having selected a point, instead of using that point as the basis for succeeding comparisons, the program chose the next following point. The fix was easy -- as it happened by removing a line from the program -- and the misbehavior was eliminated.

This is my point: I am as certain as a man can be that the noted misbehavior will never recur in that program for that reason, and I don't have to run it five years to convince myself, either.

Over the years I've tackled thousands of software bugs and noted that they divide into two fundamental classes: those that I hoped I'd fixed and those that I knew I'd fixed. I've seldom been wrong about the latter but often about the former. In retrospect in seems to me that all of the latter were in code that I'd written myself. Maybe Mr. Thomas's "software rot" would be less evident if the original writers were held responsible for quality throughout the life of the code. Maybe that's where we ought to have a law!

Properly maintained software -- by the original writers -- asymptotically over time approaches faultlessness of execution and design. The reason for this is that truly fixed bugs stay fixed. Of all control logic media, only software exhibits this characteristic.

That is, when we let it. In practice we never let that approach continue for very long before all must be redone to fit the next generation of hardware. rLs

Re: Computers and Safety

John (J.G.) Mainwaring <RM312A@BNR.CA> Fri, 7 Sep 90 15:42:00 EDT

In his otherwise well rounded summary in <u>RISKS-10.32</u> of the computers, complexity and safety discussion, Bill Murray raises the question of GOTOs, admitting that it will probably be a red rag to someone. I happen to be feel bullish on GOTOs at the moment, so here goes.

I don't for one minute dispute Dijkstra's original thesis that GOTOs can be replaced by other control structures, and they allow the creation of programming monstrosities. Deeply nested IF/THEN/ELSE and loop constructs are also error prone. In C (which many people mistakenly believe to be a programming language), BREAK is probably a worse time bomb than GOTO as programs are maintained and modified, because the target of the branch is not explicit. Of course BREAK and also RETURN from the middle of a subroutine are actually forms of GOTO. Before using any of them, it's worth examining the whole page to see if the flow of control can be improved. However, some strategies such as introducing new control variables may increase complexity of the program rather than reducing it.

There is a parallel with the attitude of British Rail to safety as quoted by Brian Randell in <u>Risks-10.31</u>: if the machine is built not to fail, you don't have to worry about the operator. Of course programming languages should be designed to avoid as many programmer pitfalls as possible. GOTO is a dubious construct. So are razors, but many people use them every day. Changes in design, caution in use, and readily available bandaids make them an acceptable risk to society.

If we want safer computer software, we will have to concentrate on formation of programmers. You can train people to keep their fingers away from the pointed end of a chisel and not to drive screws with it, but it takes years to develop a cabinet maker. Likewise, you can train people what to do or not to do in a language that provides GOTO, but to get good software for safety critical applications requires the development of a body of people familiar with both the application and software technology. Of course improved software technology will help too.

A cautionary example would be the design of bridges. We now have much better methods for designing bridges than we did in the nineteenth century. Bridges don't fall down nearly as often as they used to. Nevertheless, people were willing to use bridges then, and they still occasionally get killed using them now. We should remember that the design of a bridge is an abstraction, just like a computer program. Society has learned a good deal about managing the life cycle of the bridge abstraction and the artifact derived from it. We will learn more about using computers safely over the next few lifetimes. In the meantime, perhaps the most useful function those of us who work with computers can perform, apart from maintaining high standards in our individual endeavors, is to continue to urge caution on those who, with less understanding, have become entranced with the possibilites.

Ke: Object Code Copyright Implications

Dan Bernstein <brnstnd@KRAMDEN.ACF.NYU.EDU> Thu, 6 Sep 90 02:27:44 GMT

Three further comments on reverse engineering:

1. Decompilation isn't necessary for cloning; I don't think that a good programmer gets anything useful out of decompilation anyway. So a law prohibiting reverse engineering may not have much commercial effect. (It's a shame that economic concerns demand object-only distribution.)

2. Decompilation can be very useful in, e.g., figuring out the inner workings of a virus as quickly as possible. So a law prohibiting reverse engineering may add new risks to an already dangerous world.

3. Current copyright laws have special exemptions for each different case of computer translation. A general rule like ``It is fair use to apply a translation to a copyrighted work for personal use if the translation may be defined precisely and axiomatically'' would embrace both compilation and decompilation. It would also be in the spirit of recently expressed sentiments on the unpatentability of software---and, unfortunately, nearly as contrary to current practice.

---Dan

✓ Object Code Copyright Implications (Biddle, <u>RISKS-10.24</u>)

Randall Davis <davis@ai.mit.edu> Wed, 5 Sep 90 18:01:32 edt

> 1) If object code is copyrightable, what *exactly* is it that is subject

> to the copyright? Magnetic patterns? Ones and Zeros? Source code?

Copyright covers the way information is expressed and in this case the key to expression is any binary alphabet (for which 1's and 0's are merely conventional notation). The only thing important about the magnetic patterns of course is that there are two of them. So it is in fact that particular collection of 1's and 0's (or up's and down's or left's and right's...) that is copyright.

The same thing is true of text: it's the expression (the way information is conveyed) that's copyright, not the shape of the letters nor the alphabet that's used (using a different type font or a foreign alphabet won't change anything important as far as copyright is concerned.)

> Most importantly, these people seem to be arguing that if you have (legally)

> the "fair use" right to execute the program, you may *not* have the right to

> inspect the program itself by disassembling or reverse compilation, to
 > determine how it may work in future circumstances.

> ... of course programs may be protected by other legal mechanisms which

> are not addressed here. But copyright is usually the minimum.

Copyright law (in the US and probably elsewhere) is currently unclear on the subject of reverse engineering: different lawyers argue it in different directions and the recent Lotus case stemmed in part from the uncertainty surrounding reverse engineering.

Hence in practice copyright is not invoked to deal with it: contract law is. Most code is sold under the explicit agreement that it will not be reverse engineered. You agree to that under most shrink wrap contracts.

K Re: Accidental Disclosure of non-published phone numbers

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Wed, 05 Sep 90 10:13:01 PDT

In <u>RISKS DIGEST 10.29</u>, Peter Jones provided an excerpt from a Bell Canada mailing that warned that, when calls are billed to other than the calling phone (i.e., collect calls), the calling number is given to the billed number. The mailing stated that "this is necessary because the customer being billed must be able to verify whether or not he or she is responsible for the charge."

While I agree with this practice, I question the use of the words "necessary" and "must". What sounds like a logical requirement is in fact merely a practice of North American culture. I don't think it is common worldwide. In particular, as I recall from living in West Germany, residential phone bills there are completely unitemized, they simply say: "Pay this amount." If you think your bill is out of line, you dispute it, and the (govt. run) phone company double-checks for you. Not a great system from my (American) point of view, but it proves that is merely a matter of managing people's expectations, rather than a question of necessity and requirement.

IJ



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mon, 10 Sep 90 13:39:09 PDT

Last August, a note posted to info-vax@kl.sri.com showed how user-mode code can crash a RISC (reduced instruction set) architecture machine. The program generated a string of random bytes and jumped into it. Further discussion showed that several RISC architectures could be crashed, but none of the CISC (complex...) architectures that were tried. One person, commenting on

this, noted that one of the ways to speed up RISC architectures is to allow certain (possible) instruction sequences to have undefined behavior, and to let that behavior include "wedging" the machine. However, CISC architecture specifications make sure that every possible instruction (i.e., every pattern of bits that can be loaded into the instruction register) returns the machine to a known -- viable -- state.

Something else to lose sleep over...

Martin Minow

RISKS of relying on hardcopy printers (Voyager)

Tom Neff <tneff@bfmny0.bfm.com> 10 Sep 90 05:48:07 GMT

Although plain old hardcopy is often an excellent backup for reducing the RISKS of losing magnetic storage, it's not foolproof, as seen in this excerpt from the regular Jet Propulsion Laboratory (JPL) space probe status bulletin:

> Voyager Mission Status Report September 7, 1990

> > Voyager 1

...On August 27 Computer Command Subsystem A004 (CCSL A004) began execution. Upon arrival for the prime shift on August 27 it was discovered that five character printers in the real-time area were not printing due to one cause or another; four of the printers were either not loaded correctly or were configured in the "local" vs "online" mode and one printer had a paper jam. All of these printers were missing data since early August 25. One of the character printers that was not functioning was the General Science printer. The hard copy was needed for analysis of the PRA POR event. ...

Manalog vs digital failure modes and conservation laws

Jerry Leichter <leichter@lrw.com> Sun, 9 Sep 90 00:35:31 EDT

The recent discussion of the apparent inherent dangers of digital control control systems reminds me of a story told in another context - but which I think embodies an interesting kernel of truth. If I remember right I heard this from Bill McKeeman a couple of years back. He was called in to consult on a bank account control system, the development of which was way behind schedule. In talking to the banking people, he discovered an interesting - if obvious in retrospect - dicotomy between computer people and business people. Computer people were impressed and happy with the generality and power of their systems. Hey, the same system they were using to manage bank accounts could be programmed to play space invaders! Neat, right?

The bankers found this terrifying: If a system was general-purpose and that powerful, they didn't feel they could understand or control what it was doing

to their bank accounts. McKeeman's approach was to come up with what I guess we'd today call an axiomatic/object-oriented approach: He designed a series of basic primitives to manipulate things like money, accounts, and so on. The primitives enforced, in a very transparent way, such basic "laws" as "the law of conservation of money": Money can be neither created nor destroyed, it can only be moved from place to place. The rest of the system was built on top of these primitives, and was apparently a great success.

Now consider analogue and digital devices from the point of view of "laws". One reason analogue devices tend to have more predictable behavior is that their components follow fairly constrained physical laws - and, more important, these are laws that we understand at a deep level and can work with analytically. If the total energy stored in a system is less than 1 joule, no possible failure mode can release more than 1 joule. If that system is enclosed inside of something with a certain thermal mass, no failure mode can increase the temperature outside the enclosure by more than a certain amount. And so on. Where the inherent constraints are insufficient to guarantee safety, we can add constraints fairly easily. A governer can limit the maximum speed of a rotating element, hence indirectly such things as the energy in the system.

There can certainly be catastrophic failures due to our failure to fully understand the system: We may only put a joule of energy in, but neglect the energy stored in a spring that was compressed during assembly. Let the pin holding the spring down fail and all of a sudden there may be a lot more than a joule in there. However, we have many years of experience building these kinds of systems, and we've seen most of these kinds of failures before. We also have a lot of experience making such failures very unlikely - and we can realistically compute what "very unlikely" means.

General-purpose digital systems, on the other hand, are subject to no a priori conservation laws. If I show you all the lines of code of a program except for one and ask you to bound the value of a variable in the program, you can say nothing at all. Well, there are two exceptions, and they're instructive: If the variable isn't in scope at the hidden line, any bound you compute from the rest of the code is valid (at least in a language where you can guarantee that pointers aren't passed around arbitrarily). If the language supports variable declarations with bounds, AND guarantees to enforce them, then you also are obviously in good shape. (However, few languages do this.)

This example may shed some light on why scope rules are so important: Our programming languages continue to emphasize power and generality, not conservation laws. Scope rules (and, every once in a while, bounded variable declarations with appropriate support) are about all our languages, as such, provide us with.

Now, the algorithm being executed itself provides constraints. But there's a problem here: If the only source of constraints is the algorithm itself, an error can easily render both the algorithm and the constraint enforcement invalid. Constraints so closely tied to what is being constrained don't add safety. Relying on them is like relying on a system that suspends a weight on a string that can only hold five pounds and then saying "Well, it won't drop the weight because I KNOW that if the weight were heavier than five pounds the string would break."

Instead, constraints have to be programmed in explicitly. This is all too rarely done: Because the underlying system is so general, there are just SO many constraints to check. In an analogue system, many of the constraints come free because of the physical laws governing the parts of the system.

Beyond that, analogue systems are usually built of standardized parts - and those standardized parts are specified to obey certain fundamental constraints. We have relatively few standardized digital components, and often the constraints on them aren't very useful: They are themselves hard to check.

-- Jerry

Analog vs digital reliability

Jack Goldberg <goldberg@csl.sri.com> Mon, 10 Sep 90 10:50:09 -0700

Several correspondents have suggested that digital computers are less reliable than analog computers because of certain intrinsic properties of the two methods; for example, analog computing is more continuous, while digital computing is subject to arbitrary redirection at every step, also, the complexity of digital circuitry makes it more prone to failure. This is an interesting conjecture, but as stated it allows a confusion of design and implementation issues. Some analog realizations (cams, gears, relays with heavy armatures, etc.) do have certain reliability enhancing properties such as continuity of state during loss of drive power, or known reset states in the absence of power, but these properties do not extend to more common (and higher speed) analog realizations.

Function for function, the design of a program that realizes a standard analog function, e.g., integration or filtering, is about as easy to get right as its analog counterpart, and its implementation in digital hardware may be even more reliable (considering, for example, drift and noise in analog electronic circuits and the sharing of services in multiple-function systems that is possible in digital designs).

The real risk in using digital rather than analog computing may be that in pursuit of enhanced system functionality, one can easily introduce complex decision functions (with all their opportunity for design error) that would be infeasible in analog computers. In other words, the reliability benefit of analog design may be that it does not allow the designer to attempt more complex computing functions, with their possibilities for design error. But this limitation in computing functionality may place higher demands on human operators or limit the capabilities of safety systems, so one has to look at the larger picture.

Ke: Software bugs "stay fixed"?

Tom Neff <tneff@bfmny0.bfm.com>

9 Sep 90 20:41:14 GMT

In <u>RISKS 10.34</u> Robert L. Smith claims that it is possible to be certain that a software bug has been eradicated without waiting for nonrecurrence, and cites an example where he traced a bug in a tablet input program to one line of code, which he removed, and now feels certain that the bug is gone.

Obviously if we consider the trivial cases -- 5 line class exercises and whatnot -- we can KNOW a bug's gone. In slightly more complex cases where we nonetheless retain complete control over the code, we can stay pretty near certainty that a bug is gone. I'm sure most RISKS readers encounter this sort of thing weekly. You may not in all cases be absolutely certain you've fixed everthing wrong, but the RISK of missing something is deemed acceptable because further testing awaits.

But now take the case of truly HUGE projects, and truly old ones: the fertile spawning grounds for RISKS incidents the world over. How can we be sure we have fixed a bug? Suppose a "J" appears somewhere in a report and they task me to fix it. I find a typo in someone's module, featuring just such an errant "J" in a constant string. I correct the line. Have I fixed the problem? Anyone who thinks they can be certain without rerunning the report is in the wrong line of work. I have seen the "impossible" happen with fair regularity! For instance: Yes I fixed the line in FROBOZZ.FTN, but what I didn't know is that FROBOZZ is automagically regenerated by a code generator once a month from a config file somewhere! Next month, the "bug" reappears. Or -- I corrected my copy, but what I didn't know is that 6 other programmers have "boilerplated" from this code to do their own projects, so that not one but dozens of errant "J"'s appear in various reports. It's fine for me to feel righteous about having fixed the ONE instance originally noted, but when the customer keeps seeing "J" it's impossible to convince him we really fixed the bug! And so on -- a hundred ways for human nature to conquer seemingly iron clad programming "logic." That's why checking for nonrecurrence is the best way -- prediction is great, but observation pays the bills.

Ke: Software bugs "stay fixed"? (<u>RISKS-10.31</u>)

Stephen G. Smith <sgs@grebyn.com> Sun, 9 Sep 90 21:55:15 -0400

My experience with "bit rot", where previously solved problems reappear, is that they are usually caused by poor configuration control. While most systems have CC tools, like sccs on UNIX or CMS on VAX/VMS, getting your friendly average programmer to use them is like pulling teeth. When management insists on use of the tools, you will find lots of log entries of the form:

 REV DATE
 USER
 COMMENTS

 1.1 10/02/89
 root
 ...

 1.2 10/05/89
 root
 ...

It seems that the preferred way of working on a large system is to simply grab a complete copy of the source code (as root so that silly protection modes don't get in the way :-) and hack away. When you get several programmers working on a section of code (not at all uncommon), it's amazing that anything at all ever works.

Add in the interaction of hardware CC with software CC and you have orders of magnitude more things that can go wrong. It's amazing the number of times that you find old software running on new hardware of vice versa.

Solutions? Programmer education. Even more important is manager education, to eliminate the "It takes too much time" objection. Telling somebody at a salary review something like "We expect our

Software bugs "stay fixed" (again!)

Martyn Thomas <mct@praxis.co.uk> Mon, 10 Sep 90 13:08:57 +0100

In <u>RISKS-10.34</u> Robert L. Smith <rlsmith@mcnc.org> replies to my comments:

: Mr. Thomas implies that it is impossible to be certain, other than by :nonrecurrence, that a nontrivial software bug is fixed. My experience :indicates otherwise.

(... anecdote about a bug and its correction removed for brevity)

: This is my point: I am as certain as a man can be that the noted :misbehavior will never recur in that program for that reason, ...

Here we have it. If the error is never reintroduced and if the distributed program is compiled from the corrected source code, then this instance of the incorrect behaviour will never recur. But what about the faulty thinking which led to the error in the first place? Is it an incorrect mental model of the design, which could have led to similar errors (with identical symptoms) elsewhere in the program? Is it a misunderstanding of the meaning of a programming construct or library call (which could also lead to other similar errors)? I believe that this is what Dave Parnas (RISKS 10:32) meant by "...if they were not *properly corrected* " (my emphasis).

Note also "as certain as a man can be" above. Unfortunately people keep asking us to quantify this statement!

But this thread has rather lost its way. It started through my attempt to counter Robert Smith's seeming argument that software was better than hardware for critical applications because hardware errors recur whilst software errors do not. Of course software doesn't display the failures that hardware does, through components wearing out, but that is a small consideration alongside the bigger issues of system complexity and costs.

Simulator classification as safety-critical

Martyn Thomas <mct@praxis.co.uk> Mon, 10 Sep 90 13:24:30 +0100

In <u>RISKS-10.32</u> Brinton Cooper <abc@BRL.MIL> writes:

:Pete Mellor and Martyn Thomas agree that
:<> You cannot expect crew to do better than their
:<> training under the stress of an emergency.
:Er...the crew are, after all, thinking humans and merely another set of
:automatons in the system. A recent (past 5 years) air crash in the mid-US was
:less disastrous than it might have been precisely because the pilot performed
:beyond his training, in a situation which he had not been expected to
:encounter. This is, after all, one of the differences between human and
:machine.

This is missing the point. Crew may indeed do better than their training, but it is surely unacceptable to use this as an argument that a flight simulator is not safety-critical. If the simulator trains behaviour which causes an accident, the accident is logically a consequence of the simulator design, not of the crew (who are behaving exactly as trained). Doesn't this make the simulator as critical as any cockpit system?

Re: Postscript virus (<u>RISKS-10.32</u>)

Robert Trebor Woodhead <trebor@foretune.co.jp> Mon, 10 Sep 90 13:35:08 JST

In re: the alleged Postscript virus reported in the SJ Mercury.

Rumors of this have been flying around the virus-hunter's network for some weeks now, and two separate vaccines have been developed; to wit, one that is added to the Laser Prep file on the Macintosh to disable the SETPASSWORD operator temporarily (until next reboot of the printer) and an after-the-fact password resetter that reads the old password from the EEPROM on the Laserwriter and uses it to reset the password (This works only on 68000 based Laserwriters, and probably only on ones using ADOBE PostScript.

After much discussion, it was generally agreed upon that these tools would not be released except on an as-needed basis, for several reasons. Primary amoungst these is that nobody has yet come up with a confirmed sighting of the alleged poisoned clip-art; thus the scattered reports of malignant graphics could in fact be isolated cases of either weird machine messups, or some jerks just downloading a line or two of PostScript.

However, it should be noted that the other major reason was that the cure may be worse than the disease, in that the number of reports of problems with Laserwriter passwords is so small that it would be dwarfed by the number of problems caused by improper installation and use of the cures, and additionally the cures can easily be perverted into new variants of the possibly spurious disease they were intended to cure. Robert J Woodhead, Biar Games, Inc. !uunet!biar!trebor trebor@biar.UUCP

Ke: New Rogue Imperils Printers

<henry@zoo.toronto.edu> Mon, 10 Sep 90 13:46:22 EDT

>... PostScript, that "surreptitiously reprograms a chip inside the
 >printers, changing a seldom-used password stored there. When the
 >password is altered, ... the printer no longer functions properly."

It's not entirely clear what is going on here -- whether the code is simply doing a password change by virtue of knowing the old password or whether it's doing it by some sneak path -- but it raises an interesting risk either way.

The password on a PostScript printer (well, in the usual implementation) is a number. It protects certain parameters of the printer that user code really shouldn't change, like communications parameters and idle timeouts. There is considerable potential for malice in knowing the password, up to and including causing hardware damage of a minor sort (the EEPROM used to store printer parameters can be rewritten only a limited number of times due to wear-out processes in the chip).

The default password as shipped is 0. Very few printer owners bother to change this. The problem is that there is significant incentive *not* to change it... because the PostScript code from a good many badly-written but legitimate applications tries password 0 and will fail if it has been changed! Typically, all the application uses it for is to set some parameters back to reasonable defaults -- whether the printer owner wants it that way or not -- but the code makes no attempt to cope with the possibility of a non-standard password forbidding such changes.

Believe it or not, there are people who will defend the idea that you should leave your printer's password unchanged so that programs can mess with its parameters however they please.

Henry Spencer at U of Toronto Zoology utzoo!henry

Re: Computers and Safety (<u>RISKS-10.34</u>)

Robert Trebor Woodhead <trebor@foretune.co.jp> Mon, 10 Sep 90 13:55:49 JST

J.G. Mainwaring discourses about GOTO's and the infamous C BREAK (as in "Here is where your program will BREAK!")

It has long been my opinion (which as we all know, carries the force of law in several of the smaller West African countries.. ;^) that the EXIT() command pioneered in UCSD PASCAL was an ideal compromise. EXIT(a) exited you from enclosing procedure "a", which made it most convenient for getting out of incredibly convoluted nested structures without making them hugely more convoluted. It was the equivalent of a restricted GOTO to the end of the current procedure, with the extra ability to exit any enclosing procedure (even PROGRAM, the whole kit-n-kaboodle). It gave you the the same abilities as 90% of GOTO use, but you always knew exactly what it was going to do, and thus it was much less dangerous than BREAK.

A nice side effect of the ability to semantically nest procedures and functions in PASCAL was that this allowed you to put inner parts of some horrifically obscure structure into sub-procedures, allowing you to exit from the inner parts but not the outer parts.

Robert J Woodhead, Biar Games, Inc. !uunet!biar!trebor trebor@biar.UUCP

SafetyNet '90 Conference Announcement

<cliff@computer-science.manchester.ac.uk> Wed, 5 Sep 90 14:58:38 BST

THE SAFETYNET '90 CONFERENCE & EXHIBITION FORMAL METHODS FOR CRITICAL SYSTEMS DEVELOPMENT Royal Aeronautical Society, 4 Hamilton Place, London Tues 16th October - Wed 17th October 1990 Registration & Coffee, 9.00a.m. - 9.30a.m.

SafetyNet, PO Box 79, 19 Trinity Street, Worcester, WR1 2PX Tel: 0905 611512 Fax: 0905 612829

SafetyNet '90 Programme Day 1 16th October

09.30 General Chair Digby A. Dyke, Editor, SafetyNet

09.40 Session 1 Chair Dr. John Kershaw, RSRE

09.50 Tutorial 1: An Introduction to the RAISE Soren Prehn, Computer Resources Specification Language International

10.40 RAISE- A Case Study of Soren Prehn a Concurrent System Computer Resources International

 11.35
 Critical Software Peter Jesty, Dr. Tom

 A Standard and its
 Buckley, Keith Hobley

 Certification
 & Margaret West, University of Leeds

12.10 Intellectual Property Dr. Mathew K.O. Lee Critical Systems BP Research Centre

14.00 Product Liability (Civil Ranald Robertson & Criminal) Issues for Partner,

Developers of Safety- Stephenson Harwood Critical Software Solicitors

- 14.35Methods for DevelopingStephen Clarke, Andy CoombesSafe Software& John A McDermid, University of York
- 15.30 Panel 1: Chair: What are the relationships Prof Bernard Cohen among standards, certifica- Rex, Thompson & tion, compliance, evidence Partners and legal liability ?
- 16.30 Panel Summary Prof Bernard Cohen
- 16.40 Closing Remarks Dr. John Kershaw
- 16.45 Close of Day 1 (Please depart by 17.45)
- 19.30 Conference Dinner Guest Speaker Le Meridien Hotel, Piccadilly, London
- SafetyNet '90 Programme Day 2 17th October
- 09.35 General Chair Digby A. Dyke, Editor, SafetyNet
- 09.40 Session 2 Chair Fred Eldridge, Rex, Thompson & Partners
- 09.50 Tutorial 2: Peter Froome and Jan Cheng Adelard A Formal Method for Concurrency
- 10.40 Application of Formal Dr. D.S. Neilson Methods to Process Control BP Research Centre
- 11.35 Proof Obligations 3: Prof Bernard Cohen, Concurrent Systems Rex, Thompson & Partners
- 12.10 Refinement in the Large Paul Smith, Secure Information Systems
- 14.00 An Introduction to the NODEN Dr. Clive Pygott, RSRE Hardware Verification Suite
- 14.35 Mural A Formal Development Dr. Richard Moore Support Environment University of Manchester
- 15.30 Panel 2: Chair: Prof Cliff Jones, What is inhibiting widespread University of Manchester use of Formal Methods ?
- 16.30 Panel Summary Prof Cliff Jones
- 16.40 Closing Remarks Fred Eldridge



<skill@qucis.queensu.ca> Tue, 11 Sep 90 15:30:07 EDT

One area in which safety and reliability of analogue systems is well-understood is railway safe working. Risks readers will certainly find L.T.C. Rolt's book "Red for Danger" interesting and instructive. It covers the development of safe working in the U.K. from the first railways to the late Sixties (my edition anyway). There are many good examples of risks unnoticed, risks fixed badly, re-appearing risks, and the work it takes to make people realize the risks and then pay the price of fixing them.

Given the long experience in the U.K with safety in railway systems, you might

wonder why accidents such as Purley happen. It puzzles me too. BR has the technology to detect, on the train, the state of trackside signals, but only uses it, in the first instance, to inform the driver. In Australia (at least NSW) signals are equipped with a small handle which pivots up when the signal is at red and contacts a trip on the brake system if a train attempts to pass it. The driver cannot subvert the systemin motion, although he can reset the system and proceed once the train has fully stopped. This can only be done from outside the train (by climbing down to the trip and manually resetting it). This seems to be much more consistent with the rest of the safe working system, where signal box interlocks are implemented by requiring two largish pieces of metal to occupy the same space for conflicting events to occur. The only failure mode here is severe deformation of the metal rods.

Of course, this kind of absolute block working is not always appropriate. In places where it is common to want to pass a red signal (dense suburban) extra arms are installed between signals. These drop in sequence at a rate which reduces the train speed to around 20 km/h. Again there is no way to go faster without overunning a raised arm.

Suburban trains have the usual dead-man's throttle handle (the throttle must be pressed down continuously for it to work on the brakes not to be applied), but long distance diesels have a vigilance button which must be pressed every sixty seconds to keep the brakes off. It's a good thing that brakes are applied automatically because it is commonly believed that old hands can press this button even when sleeping. I've observed the automaton-like way that drivers press this button and I have no doubt that it happens. So I remain surprised that BR didn't seem to believe that train crew vigilance could be a problem.

Mind you, it all seems very safe compared to Canada where express passenger trains are managed using CTC and walkie-talkie radios. I've seen passenger trains following one another, separated by a few hundred yards, and relying purely on the vision of the driver in the second train. Authorized by radio, no hardware protection.

-David Skillicorn

Re: BMW Heading Control System

BANGS A L <abg@stc06.ctd.ornl.gov> Tue, 11 Sep 90 09:57:21 EDT

Michael Snyder's message about the Road Runner problem, i.e., that the system may not be able to cope with roads that go into mountains, can be a serious one. If people rely on the system enough that they tend to take their hands of the wheel and stop watching the road, then they could get in big trouble if they suddenly come to a construction site. Especially if they are moving along quickly in their BMW :-)

In other words, if the system is good enough to give people confidence, but is not good enough to deal with all possible situations, then it is risky.

Alex L. Bangs, Oak Ridge National Laboratory/CESAR, Autonomous Robotic Systems

Ke: Robustness of RISC architectures (Minow, <u>RISKS-10.35</u>)

Andy Glew <aglew@dual.crhc.uiuc.edu> Wed, 12 Sep 90 10:57:51 CDT

>Last August, a note posted to info-vax@kl.sri.com showed how user-mode >code can crash a RISC (reduced instruction set) architecture machine. >[...] several RISC architectures could be crashed, but none of the CISC >(complex...) architectures that were tried.

Let's dispose of the supposition that this is a RISC/CISC issue. Arne Helme <arne@sfd.uit.no> reposted "crashme" to the comp.arch newsgroup, and obtained a flurry of reports:

80386, '386 protected mode unix => system crash Peter da Silva 80386, '286 protected mode unix => system crash Peter da Silva DG Aviion (88K), DG/UX 4.30 => no crash ? decsystem 5200 Ultrix V3.1A => crash Arne Helme sun 4 SPARC station sunOS4.03c => crash Arne Helme MIPS R[236]000 RISC/os 4.50 => no crash Charlie Price Sun-3/50 SunOS 4.1 => unkillable cpu-bound process Andrew Taylor

Obviously, some RISCs crashed, some CISCs crashed, some RISCs survived, some CISCs survived.

The problem most likely is an OS bug. Chris Torek remembers the discussion as follows: "on all the machines that crashed *except one*, it was a bug in the OS and not in the chip. The one exception? A CISC."

Ke: Robustness of RISC architectures (Minow, <u>RISKS-10.35</u>)

Dave Sill, Oak Ridge National Laboratory <de5@de5.CTD.ORNL.GOV> Tue, 11 Sep 90 13:14:55 GMT

>... One person, commenting on

>this, noted that one of the ways to speed up RISC architectures is to allow
>certain (possible) instruction sequences to have undefined behavior, and to
>let that behavior include "wedging" the machine. However, CISC architecture
>specifications make sure that every possible instruction (i.e., every pattern
>of bits that can be loaded into the instruction register) returns the machine
>to a known -- viable -- state.

One person said that, but is it true? I find it hard to believe that excluding undefined behavior would necessarily exact a performance penalty. Further, another person in that same discussion said that the types of bugs causing the RISC machines to crash were typical of early hardware bugs in CISC machines too, and that the reason the RISC machines were crashing was because the simply weren't as thoroughly debugged as the CISC machines.

I don't know who's right, but both explanations seem equally plausable. It

seems premature to lose sleep over RISC robustness at this point.

Dave Sill (de5@ornl.gov), Martin Marietta Energy Systems, Workstation Support

Robustness of RISC architectures

Andrew Taylor <andrewt@cs.su.oz.au> Tue, 11 Sep 90 15:50:05 +1000

I don't believe this is a RISC versus CISC issue. The "execute-random-data" program found an *OS* bug in both our (RISC) MIPS boxes and our CISC Sun 3/50s.

On the MIPS the behaviour of some instruction in the conditional branch format is undefined. If there is an illegal FP instruction in the delay slot of such an undefined branch instruction. The FP instruction traps to the OS which determines the FP instruction is in a delay-slot and tries to calculate the branch destination. The OS routine called to do this detects the branch instruction is undefined but does the wrong thing, it calls "panic" halting the machine. Trivial to fix.

On our SUN 3/50s (running SunOS 4.1) some random code sequences result in a cpu-bound process which can not be killed. Rebooting is the only solution.

Its possible that OS bugs are more prevalent on RISCs because their OSs are younger.

Andrew

Ke: Robustness of RISC architectures

<henry@zoo.toronto.edu> Tue, 11 Sep 90 12:28:09 EDT

In fairness, it should be noted that most of these crashes appear to have been the result of *software* problems: the operating system was not prepared to cope with this bizarre situation when the hardware noticed it.

>... one of the ways to speed up RISC architectures is to allow
 >certain (possible) instruction sequences to have undefined behavior, and to
 >let that behavior include "wedging" the machine...

Very few RISC designers (none that I know of, in fact) are that stupid. Yes, RISC architectures often state that the results of certain sequences are undefined, but wedging the machine is *not* considered a legitimate result. (Not in a machine meant to support multi-user systems, at any rate; the rules are different for some of the more specialized processors.) Claims to the contrary are the result of ignorance or ulterior motives.

This is simply a question of proper design, not of RISC vs CISC. Certain early and buggy releases of a certain CISC processor were notorious for bugs in the protection system, e.g. circumstances in which a memory

fetch would be done with "system" permissions when it was initiated from "user" state, or vice-versa. This was mostly a result of the great complexity of the processor and its interactions with memory management; a similar problem would have been rather less likely on a RISC machine. So it cuts both ways.

>... CISC architecture

>specifications make sure that every possible instruction (i.e., every pattern >of bits that can be loaded into the instruction register) returns the machine >to a known -- viable -- state.

It is necessary to understand that "known" and "viable" are two different criteria, analogous to the frequently-mentioned-on-Risks distinction between correct functioning and safe functioning. It is not necessary that the result of violating the rules be precisely defined and the same for all variants of a particular architecture; what is required is merely that none of the possible results endanger system integrity.

Henry Spencer at U of Toronto Zoology utzoo!henry

Ke: Robustness of RISC architectures (Minow, <u>RISKS-10.35</u>)

Peter Holzer <hp@vmars.UUCP> 11 Sep 90 16:56:22 GMT

This was shown to be a OS bug on the DECstations (The OS could not correctly resume a process that trapped just after a delayed branch and instead of killing the process panicked). One person also reported that his 386 (a CISC processor) could be crashed with the same program (He did not say which UNIX he used, however. My 386 running 386/ix did not crash).

And talking of VAXes. You can crash a VAX under ULTRIX by loading the frame pointer with a negative value and then trapping into the OS.

Peter J. Holzer, Technische Universitaet Wien hp@vmars.tuwien.ac.at!uunet!mcsun!tuvie!vmars!hp

Ke: Robustness of RISC architectures

Robert Cooper <rcbc@cs.cornell.edu> Tue, 11 Sep 90 16:08:59 EDT

Many RISC architectures have a notion of a well-defined instruction stream, and undefined instruction sequences may exhibit undefined behaviour. Whether this is a real RISK, as usual, depends on a host of other factors and assumptions relating to the total system of which the RISC processor is only a part. Here are a few that come to mind:

o You are not supposed to write (much) assembly code on a RISC. Therefore if the compiler is "safe" (i.e. never generates illegal instruction sequences) , and object code is protected read-only, executing undefined

instruction sequences is unlikely. Note that a "safe" compiler need not be correct. This idea is not new: these assumptions were necessary for the B5000/B6000 series of Burroughs computers of the '60s which had unsafe user-mode object code but relied on certified compilers.

- o If the processor is used in a single user application (e.g. an embedded application) then there is little difference between just the application program failing and the whole processor failing. Both may result in byzantine failures for instance.
- o One can question the complexity needed for operating system and compiler software as a result of the RISC approach. OS code must perform much more work on traps and interrupts than on a typical CISC machine, and compiler optimizations are required to realize most of the performance benefits of RISC. Clearly these are not impossible requirements but my experience suggests that it takes several years *after* a RISC machine is introduced for the OS and compiler software to become robust.

A particularly bad scenario could be a multi-user university computer that is used for a student compiler writing course and for payroll! -- Robert Cooper

Ke: Robustness of RISC architectures

Dik T. Winter <dik@cwi.nl> 11 Sep 90 23:46:17 GMT

Martin Minow writes about a program consisting of random bytes: > Further discussion > showed that several RISC architectures could be crashed, but none of the > CISC (complex...) architectures that were tried. There was more than one report of a CISC machine that crashed. The blame

There was more than one report of a CISC machine that crashed. The blame was lain by some at the (possibly undefined) behaviour of some instruction sequences of RISC machines, but no proof was given. It is much more likely that the machines crash because of bugs in the operating system. (I know at least one sequence of bytes that will crash a Sun 4 in some situations, but I also know that it is due to an OS bug.)

The risk is obvious, one part of the system gets the blame, while nobody looks at the remainder of the system.

dik t. winter, cwi, amsterdam, nederland dik@cwi.nl

[There seemed to be enough novel in each of the preceding 7 messages that they are all included. I hope you are not all suffering from the bRISC fRISC. RISKS OF RISCs, I guess... PGN]

Re: Computers and Safety (<u>RISKS-10.34</u>)
Peter Holzer <hp@vmars.UUCP> 11 Sep 90 16:11:29 GMT

Robert Trebor Woodhead <trebor@foretune.co.jp> writes:

>J.G. Mainwaring discourses about GOTO's and the infamous C BREAK >(as in "Here is where your program will BREAK!")

>It has long been my opinion (which as we all know, carries the force >of law in several of the smaller West African countries.. ;^) that the >EXIT() command pioneered in UCSD PASCAL was an ideal compromise.

>EXIT(a) exited you from enclosing procedure "a", which made it most >convenient for getting out of incredibly convoluted nested structures >without making them hugely more convoluted. It was the equivalent of >a restricted GOTO to the end of the current procedure, with the extra >ability to exit any enclosing procedure (even PROGRAM, the whole >kit-n-kaboodle). It gave you the the same abilities as 90% of GOTO >use, but you always knew exactly what it was going to do, and thus >it was much less dangerous than BREAK.

I do know what break does: It gets me out of the enclosing switch statement or loop. This is much less powerfull then EXIT, which does not just leave this procedure (like C return) but eventually other procedures as well, which is more than you can do with goto in C (You would have to use setjmp/longjump) to do this.

Comparing EXIT with break does not make sense. It is a generalized return (Handy with those nested procedures you have in Pascal).

The danger of break is not that it leaves the switch or loop, but that you can leave it out were it would belong:

```
switch (a) {
case A:
   /* code */
case B:
   /* more code */
   break;
default:
   /* even more code */
}
```

Now should there be a break just before 'case B:' ? You have to understand the algorithm to answer the question.

This can happen with EXIT just as easily.

Peter J. Holzer, Technische Universitaet Wien hp@vmars.tuwien.ac.at!uunet!mcsun!tuvie!vmars!hp

Ke: Software doesn't wear out?

"FIDLER::ESTELL" <estell%fidler.decnet@scfd.nwc.navy.mil> 11 Sep 90 08:23:00 PDT

Software doesn't wear out? Doesn't that depend on your definitions?

Example: I use a program, duly protected by both copyright, and trade secret (of portions not disclosed in the copyright process). I use that program under terms of a valid contract. The program quits working some first of a month, because the contract has expired. I order up a new copy. When it comes, it is *not* necessarily backwards compatible with my extant data files.

Now, is my program "broken" [worn out] or not? It may function well by the *current* definitions of the vendor; but it does not get my work done any longer. (At least, not until I "make the problem fit the new too.") That sounds like a car that won't start, or run; but no, the trouble is *not* covered by the 5/50 warranty either. Sorry. (Or, perhaps better analogy, the car won't run; and the necessary repair part is no longer made.)

Apparently, "failure" has varied appearances, in the eye of the designer, (and perhaps the programmer), the vendor, and the user.

Bob

Ke: Software bugs "stay fixed" (<u>RISKS-10.33</u>)

peter da silva <peter@ficc.ferranti.com> Sat Sep 8 11:15:29 1990

- > extraneous code he doesn't understand, doesn't see how it could work, or
- > whatever and in an attempt to clean up the program, deletes or changes
- > it. This turns out to be programmer A's bug fix, and the old bug is
- > reintroduced.

In this situation it seems likely that Programmer A merely covered up or made allowances for the bug. A real bug fix would have redesigned the code so the condition that equired the obscure code didn't occur. The original comment is that fixed bugs stay fixed. Patched bugs can (and often do) resurface.

Search RISKS using swish-e

Peter da Silva +1 713 274 5180. peter@ferranti.com

Report problems with the web pages to the maintainer

┥ 🛖 🕨 🕤 🧭 😽 🚀 .



Expert system in the loop

Martyn Thomas <mct@praxis.co.uk> Thu, 13 Sep 90 18:23:50 BST

According to Electronics Weekly (Sept 12th, p2):

"Ferranti will study for MoD the feasibility of integrating a knowledge-based expert system into naval command systems, to advise commanders in battle.

"The system would reduce the risk of mistakes [sic] because battle situations are too complex for a command team to appreciate properly in the short time available. [...] If a trial system is built, it will be installed in a type-23 frigate. "

So: the battle situation is too complex to understand. The expert system is likely to be too complex to understand, too. The commander is unlikely to ignore the advice of the expert system, unless it is clearly perverse. This means that the decision (say, to launch a weapon) is being taken, in practice, by the expert system.

Is there no way we can stop this trend towards automated launch systems, before it becomes completely uncontrollable? It would be a good subject for an international treaty, even though it would be hard to find a way to verify compliance. The Aegis system on the USS Vincennes led to the death of several hundred people when a civil airbus was shot down, on a scheduled flight, in weather conditions where the aircraft would be clearly recognisable from the bridge of the Vincennes through binoculars. That tragedy was ascribed to the poor user-interface of Aegis, combined with an atmosphere of eager tension on board which made a decision to fire more likely. How can we stop people building ever-more-complex decision-support systems, and thereby losing their ability to take decisions themselves?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

×

Dave Parnas <parnas@qucis.queensu.ca> Wed, 12 Sep 90 23:24:14 EDT

Although I found the discussion of railway safety mechanisms interesting, the most interesting question for me was why the systems described would be considered "analogue". There seems to be an implicit assumption that anything that is not computerised is "analogue".

Conventionally analogue systems are those in which there are an infinite set of stable states, e.g. systems of springs and weights, electrical networks comprising resistors, inductors, capacitors, etc. Digital systems are constructed of components that have been designed to have a relatively small number of stable states with the transitions between those states being so rapid that the time spent in other states is negligible. The most common instances are binary, two stable states, but other numbers have been tried. For example, old telephone switches often used relays with 10 stable states. These were actually hybrid systems because, when the relays were in one of their stable states, analogue signals were conducted between the two subscribers.

Strictly speaking digital systems do not exist. Relays, flip flops etc are actually constructed of analogue components, only by ignoring the time in which the circuits are changing between "stable" states. However, the circuits are designed so that one can ignore those times. The transition time determines the clock rate for those systems. Subtle hardware bugs often occur when, because of poor design, the transition times are ignored when they should not have been.

The description of the railway safety systems makes them sound like digital systems made of old-fashioned technology. The little arms that were described are considered to be either "up" or "down"; one neglects the time in which they are moving between those states. The buttons described are either depressed or released; one neglects the time in which they are between those two positions.

The switches are designed so that they are either "on" or "off" and good switches are designed so that we can neglect the times when they are in an "in between" situation. It is important not to assume that "mechanical" is an antonym of "digital".

Looking back at the earliest digital computers one finds that they were made of mechanical components not unlike those described as current railway technology. If we are going to look for examples of large analogue systems, I think we have to look elsewhere. The servomechanisms used in speed control on most vehicles, and for flight surface control on aircraft, would seem better candidates.

Of course, just as the digital components are actually approximated by analogue elements, those analogue systems can now be approximated by digital systems. In those approximations the number of stable states is so large, and they are so close in some topology, that one neglects the fact that it that the number of states is finite and neglects the "gaps" between them. Here too, we have a rich source of subtle bugs.

Ke: Analog vs digital failure modes and conservation laws

Rob Sartin <sartin@hplcip.hpl.hp.com> Tue, 11 Sep 90 11:37:28 PDT

>we'd today call an axiomatic/object-oriented approach: He designed a series >of basic primitives to manipulate things like money, accounts, and so on. The >primitives enforced, in a very transparent way, such basic "laws" as "the law >of conservation of money": Money can be neither created nor destroyed, it

One can only hope that such a system would not (or would depending on your views on controlling the economy) be used at the Federal Reserve.

Rob Sartin, Software & Systems Lab, Hewlett-Packard hplabs!sartin 415-857-7592

Analog vs digital reliability (Wolitzky, <u>RISKS-10.33</u>)

David Murphy <dvjm@cs.glasgow.ac.uk> Wed, 12 Sep 90 09:15:35 BST

> Might as well carry this nit-picking one level further. As long as
> your computer's transistors, capacitors, or whatever rely on electrons,
> photons, or other quantum-mechanical wave/particles with discrete
> states, you are justified in considering them to be digital. But this
> is all silly -- the implementation is irrelevant. If you can treat
> the computer as a black box that behaves digitally, why not label it
> as such?

And therein lies the risk. One cannot always treat 'digital' systems as digital because, as many posters have pointed out, mother nature will sometimes find ways to let you know your abstraction is unsound. One of my favourite examples is Jefferies' ``Bifurcation to Chaos in clocked digital systems containing autonomous timing elements'' (Phys. Let. A,

Vol 115, No 3) where a deterministic communications protocol between two simple `digital' systems is shown to display chaos; this underlines the point that even if you start with two systems that display nice finite easily-abstracted behaviours their composition may not.

Another point that is often neglected is that many of the things we assume exist in the digital world are, in fact, forbidden. It is completely impossible to build a fair arbiter or synchroniser for instance; the axioms that should hold for such a beast are mutually contradictory; no continuous system can behave that way. Thus there will come a time in every digital design when certain questions will remain unanswered until we move outside the digitial paradigm, questions like 'how fast will it run ?' (meaning 'how fast will it run with a failure rate small enough that my customers won't notice'). There is no doubt that asynchronous design in a clocked digital paradigm will only work with some constraining assumptions about how quickly those `asynchronous' signals are actually likely to appear. And since the real world is asynchronous, -- there is no such thing as an isolated computer, -- this means that any digital design technique is just a way of improving engineering confidence in the product, not of guaranteeing correctness.

Mathematication Mathematication

John H. Whitehouse <al357@cleveland.freenet.edu> Wed, 12 Sep 90 22:47:20 -0400

In recent weeks, the risks forum has seen much discussion of software certification and of the relative risk of digital vs. analog computing. I would like to suggest another realm of discussion which relates to the notion of software certification. Specifically, I would like to see some discussion here of the value of certifying software professionals. In this regard, I refer to those certification designators administered by the Institute for Certification of Computer Professionals in Des Plaines, Illinois.

From its inception, our field has never been able to find enough qualified people to meet the demand. As a result, we have drafted people from a wide variety of academic disciplines. Further, many workers in our field have never even seen the inside of a university. In addition, very few universities have offered majors in computer-related disciplines until "recently", i.e. in the last 25 years. I am not trying to condemn those people now practicing in this field who lack a "proper" academic background. In fact, I will openly state that many people who do have a computer science major are unable to perform adequately in the field.

Regardless of background, some people seem to have developed an adequate understanding in this field whereas others have not. The fact that the vast majority of managers were either non-technical from the start or have become non-technical over the years means that probably the vast majority of people in this field are not receiving evaluations which reflect the actual quality of their work and the depth of their understanding. This cuts two ways. First, many poor practitioners continue to survive in the field despite their poor performance. Second, many excellent technical people fail to receive proper reward for their accomplishments.

Hiring is expensive and usually done pretty much in the blind. Firing is risk-laden in our litigious society.

It is my contention that the vast majority of software defects are the product of people who lack understanding of what they are doing. These defects present a risk to the public and the public is not prepared to assess the relative skill level of software professionals.

For these reasons, I favor the certification of software professionals. We have tried to bring this about for 28 years on a voluntary basis, but those who know that they could never pass make high sounding arguments to convince others that voluntary certification is not a desirable goal. Academics have not joined in the debate since they are generally immune from the problem.

I would like to hear some discussion on this issue.

[We have been around this topic before, with Nancy Leveson in <u>RISKS-5.28</u> and following discussion in <u>RISKS-5.33</u>, Appendix B of the ACARD report noted in <u>RISKS-4.14</u>, John Shore with some appropriate references in <u>RISKS-4.78</u>, and earlier discussions. Perhaps it is time to try again. PGN]

ZIP code correcting software

<BQABAA@CFRVM> Thu, 13 Sep 90 09:43:15 GMT

Several administrative departments on our campus are interested in purchasing software which claims to validate and correct ZIP codes. This could be used interactively to tell an operator that he/she is keying a ZIP code which is invalid for the given street and city information; it could also be used in batch to "clean-up" address data. Apparently the US Post Office maintains massive tables of address data which various software vendors use as the basis for these kinds of software packages.

Does anyone have experience with this kind of software? My concerns would be as follows:

- 1. What is the error rate with this process?
- 2. What happens when additions and changes are made by the Post Office to their tables but the vendor has not yet gotten the updates out to the end user of the software? Will the software keep "correcting" a ZIP code which is in fact already correct?

I've had personal experiences where some of my mail suddenly shows up with a changed (and wrong) ZIP code. After contacting the sender and getting the ZIP code changed back to what it should be, I've seen it get changed again a few months later. It's obvious to me that they are running a batch update on their mailing list using software that says my ZIP code is wrong. This seems to me to be part of a trend for people to put their faith in "error-correcting" software which can't always tell what really needs correcting.

--- Rich Meyer

Richard W. Meyer, University Computing Services, University of South Florida, Tampa DBQABAA@CFRVM.BITNET

✓ Software Bugs "stay fixed"? (Steve Smith, <u>RISKS-10.35</u>)

Jeff Jacobs <76702.456@compuserve.com> 12 Sep 90 16:19:14 EDT

>My experience with "bit rot", where previously solved problems reappear, is
>that they are usually caused by poor configuration control. While most systems
>have CC tools, like sccs on UNIX or CMS on VAX/VMS, getting your friendly
>average programmer to use them is like pulling teeth. When management insists
>on use of the tools, you will find lots of log entries of the form:

>Solutions?

The following is a description of a "solution".

(Way back in the early days of the TDRSS ground station network development...)

During my troubleshooting activities, it quickly became obvious that many of the "show-stoppers" were not "bugs", but were a combination of procedural, operational and communication problems. The large number of different test configurations, the number of different groups performing testing, and the technical inexperience of the test and configuration management personnel resulted in a chaotic situation. Although a conceptually sound set of procedures had been drafted, they were manual and paper-based, and were unable to keep up with the level of activity. An average of 4 days per month were lost simply due to errors in editing command files for compiling and linking. These were *project* months, where several dozen people would be waiting for me to resolve a "show-stopper". I would spend enormous amounts of time trying to resolve what software was in use, how it was used, etc, etc. Furthermore, it was almost impossible for management to determine the status of fixes, enhancements and updates to the software.

The situation was quite amenable to automation. Although my initial proposal to TRW was turned down, I proceeded to create an initial version for my own group's use; we were making "quick-fixes" at a rapid rate, and needed the support that the tool would provide. The tool, called the "Fix Processor", was completed in six weeks. It is effectively an expert system, built using Object Oriented and AI techniques in a Lisp-like language. (It was described in a prize winning paper, "Utilizing Expert Systems to Improve the Configuration Management Process", by Sherri Sweetman, George Washington, University, for the Project Management Institute).

This is **NOT** a "version control" system; it is much more complex. Software

"fixes" (including updates and enhancements), migrated physically. Initially, all software resides in controlled baselines on development machines. As developers made changes to a given task, code was taken from the baseline and moved to work areas. As it went through various stages of testing and acceptance, it transitioned to physical control of other groups. Prior to a delivery to WSGT, all accepted changes would be "rolled" into a new baseline and the entire process would start over.

The Fix Processor was initially used by the various integration and testing groups. Once its effectiveness was proven, it was also propagated to the development groups, who, although initially opposing it, soon became its strongest advocates!!!

Features of the Fix Processor included:

- Automated the tedious, time consuming and error prone operations required to transition a piece of software. This includes creation of new directories, copying files, generation of command files, etc., all of which formerly had to be performed manually. This was crucial to the widespread acceptance and use of the system.

- Separated compiling and linking of new fixes from actual incorporation into testing configurations. (Tasks had to compiled and linked prior to actual testing. It was also sometimes necessary to remove a new version of a task from a test configuration).

- An on-line reporting and query facility for determining the status of software, usage in test configurations, etc. This was not only a key management tool, it also provided a means of communication between the various integration and testing groups. Problems which formerly took days to resolve were literally reduced to minutes.

- Extensive validation of user inputs and requests.

- Support and tracking for special requirements, such as debugging, "quick and dirty" fixes, etc.

- Automated collection of all approved changes into a new baseline, a process which formerly required more than a week (and was incredibly error prone).

- Co-ordinated task transitions with the necessary paper trail. (I subsequently revised the paper work system).

- Logged all activities and results into a database.

The net result of these changes was a smoothly functioning, manageable project. Mammoth turn-overs were eliminated. Software was turned over by the developers in small, manageable increments on a continuous basis (as opposed to the previous "here it all is method", which would take weeks to straighten out).

Problems were easily identified and quickly solved ; productivity and morale were immeasurably improved and the project became truly manageable.

Note that one of the key elements to the success of the FIX Processor is that

it made life *easier* for everybody involved (including me). Note also that the "automation" helped ensure that problems didn't recur, and it was quite easy to verify the complete path of software.

Jeffrey M. Jacobs, ConsArt Systems Inc, Technology & Management Consulting P.O. Box 3016, Manhattan Beach, CA 90266 (213)376-3802



Report problems with the web pages to the maintainer



Amos Shapir <amos@taux01.nsc.com> 13 Sep 90 23:13:15 GMT

Tel Aviv, Sep. 13 -

12 private investigators and a few employees of the Income Tax bureau were arrested on suspicions of bribery and breach of trust. The investigators have allegedly bribed income tax employees in return for computer data, which included details about taxpayers' income and assets. Under investigation are also suspicions that some investigators - most of them former policemen - have used the same means to receive data of police computerized files as well. As usual, the human factor is the weakest link in any security system. Luckily, in this case the data was handed as printouts; one can easily imagine what could have happened if the suspects had had their own computers and modems to contact the compromised systems directly.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522255 TWX: 33691, fax: +972-52-558322

Relatively Risky Cars

"Martin Burgess" <burgess@sievax.enet.dec.com> Fri, 14 Sep 90 04:42:44 PDT

Yesterday a program on British T.V. pointed out (again) that car buyers in Sweden and the U.S.A. can obtain information about the relative safety of different models, and that this information is not available in the U.K.

The RISKS forum would seem to be an ideal place to post the details, if the copyright laws allow.

It would also be interesting to see if there were differences between cars sold into different markets - for example, does the widespread fitting of air conditioning in the U.S.A. affect the safety of passengers when there is an accident ?

Martin Burgess

Ke: The need for software certification

Theodore Ts'o <tytso@ATHENA.MIT.EDU> Thu, 13 Sep 90 22:11:06 -0400

I am against the "certifying" of software professionals. My objections fall basically into two areas. The first is that there is no valid way to measure software "competence". How do you do it? There are many different software methodolgies out there, all with their own adherents --- trying to figure out which ones of them are ``correct'' usually results in a religious war.

For example, all computer science students at MIT are required to take 6.170 (also known as Software Engineering) as a graduation requirement. (I just graduated in June 1990; the last time this topic came up, I was afraid to air my opinions because I would shortly be applying to graduate school.) But in any case, my personal opinion of that course is that it is so completely dated that it isn't even funny. For example, the course is taught in an archaic language, CLU, instead of a more modern object-oriented language such as C++. In the class, we're told that global variables are always evil --- there's no excuse for them at ever; yet in order to build the linker (which was written in CLU), the sources turned on a magic flag so that it could have global variables to store the symbol table. I suppose the performance hit of passing the symbol table object to every single procedure in the linker was too much to handle.

We were told that the One True Way to program involved keeping a design notebook and not even trying to code until we had sketched out the whole thing in pseudo-code, which I guess is the current "in" way to do structured coding. (Remember when people said that flow-charting was the only way to write error-free programs?) When I and my fellow students in my group took the course, we used an emacs buffer as our design notebook, and our psuedo code was written in CLU itself.

Surprisingly, version control (such as RCS) was never discussed at all. I suppose the theory was that if we designed everything in pseudo-code from scratch, we would never need to rewrite or revise any of it, so version control was considered important. I will leave it to the Gentle Reader's judgement as to whether or not you can teach a reasonable Software Engineering in today's environment, when several people can be changing files on a networked filesystem, without at least mentioning version control.

Our conclusion was that the religion which was preached to us was developed in the days of teletypes and punched cards, when actually coding several different algorithms and trying them out was too expensive; when only one person could modify a file at a time because of physical limitations, so version control wasn't important; and when interactive computers were nearly nonexistent, so the only kind of One True Design Notebook was a spiral bound one.

In any case, we (the students in my programming group) didn't buy any of it. So by the deadline where we supposed to have produced a design document detailing how we would do things (and which would be used to penalize us if we deviated from it in our final implementation), we wrote an almost completely working prototype. We then wrote our design document from our implementation, instead of the other way around. We ended up with one of the cleanest implementations and received one of the highest scores in the class. In fact, we received a letter of commendation saying that we were in the top 5% of the class, and that we deserved some recognition beyond merely getting an "A" in the class.

The point of all of this? My group managed to get an A in this class without absorbing any of the religious tenets of Professor Liskov's programming methodology. (This is not to say that everything in the class was bad; but a lot of it was trash, and I had learned most of the good parts by being a student systems programmer at Project Athena, so the class was essentially a waste of time for me.) So how do you certify someone? If required to, I can parrot back all of the ``right'' answers on a written exam. Those answers would also mean very little about how I really go about my programming work. (I won't go into the flame wars about how my personal style is better-or-worse than the traditional "top-down", or whatever else is in vogue today. My style works for me --- I write generally bug-free code, and I won't dictate to you how to write bug-free code if you won't dictate to me how I should write mine.)

The second general objection that I have against the certification of software professionals is that it might very well become a guild. In my

mind, there is great danger that once you have the people who are "IN", they will try to maintain a competitive advantage and keep most other people "OUT". Mr. Whitehouse has already granted that a college degree cannot be used to discriminate those who can program well against those who do not program well. I am very much afraid that any system of software certification will be used to push one person's pet software methodology and to exclude people who don't agree with him or her.

Worst yet, it could become like many unions today, and be used to protect mediocrity within the group against people who are actually better qualified, but who aren't in the appropriate magic group. This could be extremely dangerous, if management types were to actually believe that being ``certified'' would mean that the code that person generates is "guaranteed" to be bug-free, when in fact the code might be much worse than someone who didn't have the magic blessing. Knowing human nature this is probably a more clear and present RISK than the current method which depends on the free market.

- Ted

Ke: Expert System in the loop (Thomas, <u>RISKS-10.37</u>)

Steven Philipson <stevenp@decwrl.dec.com> Thu, 13 Sep 90 16:56:27 PDT

In <u>Risks 10.37</u>, Martyn Thomas <mct@praxis.co.uk> writes about a Feranti study on the "feasibility of integrating a knowledge-based expert system into naval command systems, to advise commanders in battle".

Thomas concludes:

>The commander is unlikely to ignore the advice of the expert system,
>unless it is clearly perverse. This means that the decision (say,
>to launch a weapon) is being taken, in practice, by the expert system.

Neither conclusion follows. First, the proposed system is intended to "advise commanders". It is NOT stated that the system is intended to act on its own or to be blindly followed. Commanders will be very likely to ignore the advise of such a system -- they tend to be very wary of automated systems, and regard themselves as experts. Commanders often get contradictory advise from their human advisors. The essence of their job is to evaluate recommendations and make the best decisions that they can.

An advisory system that recommends action that is at variance with other sources will likely be disregarded UNLESS the system makes a strong case to support its recommendation. A system that cannot justify its recommendations will be of little use, as a commander can not follow a blind recommendation; he has to know the line of reasoning and facts on which the recommendation is based, regardless of whether that recommendation comes from a human or automated source.

Such a system could be of great value. IF an expert system were

to detect a trend or correlate bits of information that indicate a significant development, it could issue a recommendation and support it with the data points and chain of reasoning that were used to arrive at that conclusion. The commander could then review that recommendation and decide whether or not to act upon it given his evaluation of the validity of the reasoning. All this may not be possible to do in practice, but there is the potential for an advance here in implementing a more effective and safe decision making process.

>The Aegis system on the USS Vincennes led to the death of
>several hundred people when a civil airbus was shot down, on a scheduled
>flight, in weather conditions where the aircraft would be clearly
>recognisable from the bridge of the Vincennes through binoculars. That
>tragedy was ascribed to the poor user-interface of Aegis, combined with an
>atmosphere of eager tension on board which made a decision to fire more
>likely. How can we stop people building ever-more-complex decision-support
>systems, and thereby losing their ability to take decisions themselves?

The facts above are incorrect and/or incomplete. The Vincennes did not acquire visual contact with the Airbus nor could it have -- visibility was restricted by haze, and the aircraft was shot down before it entered visual range. The term "eager tension" is misleading -- the transcripts of the incident and investigation indicate that there was an atmosphere of tension *and fear*. It should also be noted that the Aegis system did not make a decision to fire -- that was purely a human decision based on available (albeit misinterpreted) information.

A case can be made that an automated system might have concluded from the available data that the Airbus was NOT conducting an attack, and could have *advised* the commander to NOT fire. We should keep in mind though that warnings were given by a human operator that the aircraft might be a commercial flight. These warnings were not heeded -the preponderance of information available to the commander indicated that a decision to fire was necessary for the protection of the ship.

We all wish to minimize risk, but we must recognize that we can not eliminate it; there are significant risks in human activities regardless of how they are undertaken. There will be grave errors in military operations regardless of the technology that we use.

We have good cause to be wary of automated systems in critical applications, but we should not dismiss them out of hand. Blind trust is dangerous, but so is blind distrust. It's our responsibility as computer professionals to see to it that any computer technology that is developed is done so in a way that minimizes risks, and that the end users are cognizant of the limitations and hazards associated with such systems.

Steve Philipson

Ke: Expert system in the loop (Thomas, <u>RISKS-10.37</u>)

Brinton Cooper <abc@BRL.MIL> Fri, 14 Sep 90 10:32:35 EDT Martyn Thomas reports:

>According to Electronics Weekly (Sept 12th, p2):

"Ferranti will study for MoD the feasibility of integrating a >knowledge-based expert system into naval command systems, to advise >commanders in battle.

He then objects to the use of automated launch systems, asserting:

>The Aegis system on the USS Vincennes led to the death of
>several hundred people when a civil airbus was shot down, on a scheduled
>flight, in weather conditions where the aircraft would be clearly
>recognisable from the bridge of the Vincennes through binoculars. That
>tragedy was ascribed to the poor user-interface of Aegis, combined with an
>atmosphere of eager tension on board which made a decision to fire more
>likely.

In fact, he has contradicted his own assertion that the AEgis system was responsible by pointing out the shortcomings in human judgement, human psochology, and human I/O. The principal (and significant) shortcoming of AEgis in this scenario is that its database apparently did not include a readily available schedule of commercial airline flights for the region in which AEgis was deployed.

If humans insist upon creating conflict situations where decisions depend upon evaluating large numbers of interacting variables, NOT to use automated decision support systems would be the tragedy.

He concludes:

> How can we stop people building ever-more-complex decision-support >systems, and thereby losing their ability to take decisions themselves?

So long as there are ever more complex decisions to be made, we must either improve the decision maker or give the decision maker some help.

The only other choice is to avoid the complex decisions altogether.

[Because of the nature of this topic, I feel compelled to disclaim any relationship between what I have written and for whom I work. These opinions are my own <...>]

_Brint

Ke: Computer Unreliability and Social Vulnerability: critique

Dan Schlitt <dan@sci.ccny.cuny.edu> Tue, 11 Sep 90 14:37:29 -0400

Pete Mellor <pm@cs.city.ac.uk> writes in <u>RISKS-10.28</u>: >The authors do not make it clear initially which of two different meanings of >'catastrophic' they intend: >

> a) sudden and unpredictable, 'anything can happen', and

> b) having appalling consequences.

>

>The first is a classification of the effect (which I prefer to call a 'wild >failure' to avoid confusion), and the second is a measure of the cost. For >example, when arguing that computers are inherently unreliable because they are >prone to 'catastrophic failure', they quote the Blackhawk example. The cause of >this series of accidents was eventually traced to electromagnetic interference, >as the authors state. While it is probably true that only a *digital* >fly-by-wire system would exhibit a wild mode of failure in response to EMI, it >is not until half-way down the next page, where the authors point out that >digital systems have far more discontinuities than analogue systems, that it >becomes clear that they are using 'catastrophic' in sense a), and not in sense >b).

>

It might be well to note that the natural assumption that discrete systems, such as digital ones, are more prone to wild mode failure than nice continuous analogue systems is a dangerous one. The term "chaos" has become a buzzword and as a result much of the real meaning has been lost to the world. One of the important observations was that, except for some exceptional cases, "wild behavior" is generic for conservative mechanical systems. For non-conservative systems the situation is not too different. It is only because the most familiar and most analyzed cases are special that we make the "natural" assumption of smooth nice behavior.

The unfamiliar but common case is one where a system exhibits smooth regular behavior punctuated by wild jumps to a wildly different smooth state. The timing of the jumps is highly unpredictable because it depends critically on initial conditions.

>The authors are right to claim that computer systems are too complex to be >tested thoroughly, if by this they mean 'exhaustively'. It is apparent from >their example of a system monitoring 100 binary signals that they do mean this. >

>Exhaustive testing in this sense is well known to be impossible. Even in >modestly complex systems one can only test a representative sample of inputs. >Provided the selected sample is realistic, one can, however obtain a reasonable >degree of confidence that a reliability target has been reached, but *only if >the target is not too high*.

>

This sort of exhaustive testing is also impossible for general mechanical systems. It requires good design to make a mechanical system which falls in the class of those that are well behaved. It is not clear to me why it is not also possible to use similar good design to construct sufficiently stable digital systems. The main difference between the two is the difference in the amount of design experience we collectively have had in the two cases.

Catastrophic failure in the second sense was not allowed to stop the development of mechanical systems in the past. Collapsing cathedrals the failure of the Tacoma narrows bridge or airplanes falling out of the sky did not stop architecture, bridge building or aviation

-- and bridges are still known to collapse. It would be tragic if these concerns were to halt development of digital systems.

Mellor is right that the challenge is to develop the tools for testing and analysis that are required.

Dan Schlitt, Manager, Science Division Computer Facility City College of New York, New York, NY 10031, (212)650-7885 dan@ccnysci.uucp dan@ccnysci.bitnet

✓ Large analog systems and NSW railroads

David Benson <benson_d@maths.su.oz.au> Fri, 14 Sep 90 11:21:50 +10

Having just arrived in NSW I have yet to experience the safe railroads -- but certainly recommend visiting Australia.

David Parnas comments that the railroads are not properly "large analog systems". I certainly agree. But his examples of "large analog systems" seem rather small scale stuff to those of us who think about spreadsheets, general ledger, Star Wars, and other large scale systems on or containing digital computers.

So perhaps there are no "really large analog systems." After all, the 747-400 I rode on for the 15 hour overwater flight from LAX to SYD isn't a "really large analog system", is it?

Seriously, I doubt that in the bad old days before computers that the systems in use were as safe, as reliable, or as inexpensive as in the good new days with computers. This is certainly the case for manual speadsheets, manual or semi-manual general ledger, and other inherently descrete systems often associated with accounting -- or anyway, bookkeeping. Indeed, there is something rather inhumane about bookkeeping seems far better for the spirit to relegate this task to mere computers.

I assert, without even bothering to review the data, that air travel is vastly safer post-computer (say, since 1970) than pre-computer. And so it goes...

From this casual review of nineteenth and twentieth century technology I am going to baldly state that the largest analog systems I can think of are all basically static -- such as bridges under load -- and are seriously overdesigned by the standards of this day. These standards are manifested in software, airplanes, etc.

I hope, by this statement, to generate some discussion and thus perhaps some enlightenment.

Analog vs Digital reliability

&lummer@DOCKMASTER.NCSC.MIL> Fri, 14 Sep 90 10:09 EDT

Can somebody provide a clear explaination of the role of delay in analog and digital circuits? We can attempt to compare the two by making associations such as "the voltage on an (analog) capacitor is the equivalent of the number held in a digital register". Then in the digital world we worry alot about when the register gets changed and try to prove that only one writer can exist at anytime. Analog systems don't seem to have the same concerns. Or do they? --Bill Plummer, Wang Laboratories, Inc..

Ke: ZIP code correcting software

Bernard M. Gunther <bmg@mck-csc.UUCP> Fri, 14 Sep 90 11:00:10 EDT

>Does anyone have experience with this kind of software? My concerns >would be as follows:

> 1. What is the error rate with this process?

- > 2. What happens when additions and changes are made by the Post
- > Office to their tables but the vendor has not yet gotten the
- > updates out to the end user of the software? Will the software
- > keep "correcting" a ZIP code which is in fact already correct?

I have had two sets of experiences with this sort of problem:

1 - There must exist a tape which has determined that my ZIP code 02141 is in Boston and not in Cambridge. I give my address with the the Cambridge town name, and I get letters back with Boston listed as the town name. Nothing I do seems to correct this problem.

2 - I have used a PC software package which takes street addresses and town names and plots the points on a digital map. In matching a number of bank branch locations, the success rate of this program without any human guidance is around 60-65%. Using a limited amount of inteligence, this goes up to 75-80%. Achieving 90+% requires calling the branches and getting better address and cross streets. The key limiting factors are the quality of the address given and quality of the source maps.

Bernie Gunther

Ke: ZIP code validation software

Dave Katz <katz@merit.edu> Fri, 14 Sep 90 10:27:36 EST

I recently stopped into a stereo/appliance retail outlet to pick up a \$15 accessory for which I wanted to pay cash. Being in a hurry, I tossed down exact change and gave my thanks to the salesman. Shortly thereafter, lights flashed and beepers beeped, and I was told that in no uncertain terms that I had to wait for the purchase to be entered into the computer.

My annoyance grew to anger as the salesman fumbled with the computer, apparently having difficulty even "logging in." (If it wasn't the guy's first day on the job, the store is in real trouble.) He then asked for my name and address. Not wanting to be on their mailing

list, and having real objections to giving my vital statistics away for a small cash purchase, I protested. "I have to type it in or the computer won't allow the sale." Feeling chagrined, I made up a fake name and address in an obscure town in central Michigan. The salesman dutifully typed in the phony address. The computer beeped and displayed "Invalid ZIP code." "The computer must have made a mistake," said I, feeling like an unmasked felon. The salesman looked badly confused, I got even more upset, and finally another salesman told him to enter "00000", satisfying the machine.

After all that, the item had to be taken to another counter where a sales slip was printed in triplicate, each copy separately filed, the inventory control bar code read, and the anti-theft device demagnetized. [The computer then announced that there were -5 of these items left in stock.]

Total elapsed time was nearly 15 minutes.

The risks are twofold--one being a privacy risk, and the other being the encroachment of inappropriate, excessively complex technology.

--Dave Katz University of Michigan



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Paul Eggert <eggert@twinsun.com> Fri, 14 Sep 90 12:39:44 PDT

[Reprinted from comp.parallel Usenet newsgroup (Dennis Stevenson, moderator)]
From: aglew@uiuc.edu (Andy Glew)
Newsgroups: comp.parallel
Subject: Poetic Justice in a Machine Crash
Date: 14 Sep 90 12:56:47 GMT
Organization: Center for Reliable and High-Performance Computing University of Illinois at Urbana Champaign

Our Encore Multimax just crashed in a way that seems like poetic justice:

On the console terminal appeared a fragment of somebody's paper about multiprocessor interconnection networks. The last readable sentence was:

"...it is difficult to build shared memory procesors

"^%%^\$#\$%#%\$#it is difficult to build shared memory\$%#%\$#it is difficult to "build shared memory\$%#%\$#it is difficult to build shared memory\$%#%\$#it is "difficult to build shared memory%^\$%^\$@#\$@!\$@#\$@difficult to build "shared memory\$%#\$%\$%#\$%shared memory%^\$%^\$%^ shared memory %&\$%^^%\$\$%^% "shared memory&*^&*&*^&*ashared memory

...

Almost too good to be true :-)

(The screen garbage and control characters are not recorded verbatim).

[Once again I am reminded of the prophetic nature of Vic Vyssotsky's Chaostron piece, reprinted in CACM, April 1984, pp. 356-7. PGN]

Ke: Expert system in the loop (Philipson, <u>RISKS-10.38</u>)

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Fri, 14 Sep 90 14:33:30 PDT

>The commander is unlikely to ignore the advice of the expert system,
>unless it is clearly perverse. This means that the decision (say,
>to launch a weapon) is being taken, in practice, by the expert system.

This remark incited two responses asserting that the retaliatory decision in the case of the Vincennes was a matter of human, not mechanical, judgment, and that the computer system merely provided humans with better information than they would otherwise have, so that the human decision becomes more meaningful. This is ridiculous.

In the case of the Vincennes, it cannot be disputed that a mistake was made. The Pentagon found no human responsible for it, so it must have been a mechanical error. (Recently, Captain Rogers was awarded a special medal of honor for his courage in commanding the Vincennes through the shootdown.) The assertion that humans have time to meaningfully evaluate the computers' information in a few minutes is patent nonsense (as proven by the Vincennes) - all humans can do is to *gamble* whether the computers (or their readings of the computers' consoles) are right, and so they act as no more nor less than randomizing agencies - i.e. one would get the same level of "judgment" by card shuffling.

Such decisionmaking is de facto *governed* by computer: without computer prompts, no retaliatory decision at all would be taken; and, simply because of computer prompts, a virtually immediate retaliatory decision is mandated; and, that decision is based fully

on the information provided by the computers.

In view of these circumscribing facts, the construction that in practice computers "make" the controlling decisions is required both as a matter of common sense and as a matter of law, under the realistic interpretive standards unhesitatingly applied by the Supreme Court in Bowsher v. Synar, (1986) 106 S.Ct. 3181-3191, which ruled that the facial freedom of a proposed officer's decisionmaking was nullified by the circumscribing constraints:

To permit the execution of the laws to be vested in an officer only answerable to Congress would, in practical terms, reserve in Congress control of the execution of the laws... There is no merit to the contention that the [officer] performs his duties independently and is not subservient to Congress. Although nominated by the President... the [officer] is removable only at the initiative of Congress... the political realities do not reveal that the [officer] is free from Congress' influence... [a] though he is to have 'due regard' for [executive rulings]... The congressional removal power created a 'here-and-now subservience' of the [officer] to Congress... In constitutional terms, the removal powers... dictate that he will be subservient to Congress . . . Unless we make the naive assumption that the economic destiny of the Nation could be safely entrusted to a mindless bank of computers, the powers that this Act vests in the [officer] must be recognized as having transcendent importance.

Just so, minimal retaliatory timelines "in practical terms" assure the dominance of military computers in Vincennes-style decisions, which gives rise to a "here-and-now subservience" of military to to mechanical bodies.

Re: Expert system in the loop (Philipson, <u>RISKS-10.38</u>)

"Peter G. Rose" <CO114@URIACC.BITNET> Fri, 14 Sep 90 14:26:51 EDT

>From: stevenp@decwrl.dec.com (Steven Philipson)
>In <u>Risks 10.37</u>, Martyn Thomas <mct@praxis.co.uk> writes
<>The commander is unlikely to ignore the advice of the expert system,
<>unless it is clearly perverse. This means that the decision (say,
<>to launch a weapon) is being taken, in practice, by the expert system.
>

> Neither conclusion follows. First, the proposed system is intended >to "advise commanders". It is NOT stated that the system is intended >to act on its own or to be blindly followed. Commanders will be very >likely to ignore the advise of such a system -- they tend to be very

There is truth in both these viewpoints. My observations indicate that people tend to place more faith in the 'judgment' of machines than is warrented.

Steven believes that commanders are suspicious enough of expert systems that this tendancy is overridden. The real issue is getting good information to the person making the decisions, (Can you tell I'm M.I.S.?) and making sure that the decision maker understands the system(s) that is(are) giving him information well enough to evaluate that information.

Most of the problems I've seen with automated systems aren't intrinsic to the form. They're implementation errors.

* When you put in your 'Expert System', do you train the user to evaluate its output, or do you train them to follow its directions? If the people who MAKE the system are the ones doing the training, I'd bet on the latter.

* Does the system tell you WHY it thinks you should do something, or does it just tell you to DO it?. Deciding what a person does and does not need to know is always a tricky task.

* Is it obvious or explained HOW the system works? It's much easier to predict bizzare, erroneous, or just less-than-optimal performance if you've got a good idea of how the system works.

* When you put the system in, are you removing other sources of information? Putting a tv camera on a vehical will let you see into blind spots, zoom, and edit in other information. That DOESN'T mean you ought to plate-over the windshield....

The problems we have using technological artifacts are the same as we have making the parts work in the artifact. The pieces have to work with the system, And the system always includes all the parts AROUND whatever you're changing.

Ke: Expert system in the loop (Philipson, <u>RISKS-10.38</u>)

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Fri, 14 Sep 90 10:35:57 PDT

> We all wish to minimize risk, but we must recognize that we can
 > not eliminate it; there are significant risks in human activities
 > regardless of how they are undertaken. There will be grave errors
 > in military operations regardless of the technology that we use.

The captain of the Vincennes was faced with a decision that had four possible outcomes:

- 1. Destroy approaching plane; plane is hostile (CORRECT OUTCOME)
- 2. Destroy approaching plane; plane is not hostile (ERRONEOUS OUTCOME)
- 3. Don't destroy approaching plane; plane is hostile (ERRONEOUS OUTCOME)
- 4. Don't destroy approaching plane; plane is not hostile (CORRECT OUTCOME)

Mr. Philipson's statements read as if erroneous-outcomes such as case #2 are unavoidable given the nature of decision-support systems and human decision-making, and are qualitatively similar to errors such as case #3. They are neither. Military personnel have, by joining or accepting induction into armed service, accepted certain risks. Civilians have not. If there is any doubt whatsoever that the approaching plane was hostile, the Captain should have decided not to destroy it, accepting the risk of outcome #3, i.e., that his ship might come under attack (Note: not even necessarily that his ship or crew would sustain any injuries). He and his crew signed up for that risk when they went to sea. The passengers of the airliner had accepted no such risk. The Captain should have waited.

Jeff Johnson, HP Labs, Palo Alto

🗡 I'm 99% Sure You're A Crook!!!

<mmm@cup.portal.com> Fri, 14 Sep 90 13:59:54 PDT

The following items appeared in the 9/14/90 edition of Action Line, a consumer advocacy department of the San Jose-Mercury-News.

I recently shopped at PW Market at Landess and Morrill roads. When I gave the clerk my check, she immediately accused me of writing a bad check -- several, in fact. I was totally embarrassed. I've never bounced a check in my life! -- L.T.L., San Jose

[Response by Action Line.]

There was a communication problem, says Mike McMaster, store manager, who says he's sorry you were embarrassed. He will be sending you a letter saying so. However, McMaster says you weren't accused of writing a bad check but misunderstood the chain's check-clearing system, which is different from most other stores'. PW's system records bad checks by listing the last six digits of the checking account number; the _complete_ checking account number is listed in a separate booklet. The last six digits of your account number matched one in the store's computer, which is what caught the clerk's attention. After the clerk checked the book, however, she realized the rest of your account number did not match. McMaster says you didn't want to listen when employees tried to explain it to you. McMaster says PW is trying to rework its computer system so it will accept 10-digit numbers to avoid a similar situation in the future.

[To me, it seems like there is quite a range of quality in the machines used to verify my credit. Some are solid-looking hardware from NCR or IBM with expensive keyswitches and plasma displays. Others are cheapo stuff with LED displays and calculator-style keypads. I guess PW went with the system from Ma & Pa Kettle POS Systems. mmm]

A Nightmare: Security compromise with SUN's C2 package

Caveh Jalali <caveh@csl.sri.com> Mon, 17 Sep 90 15:21:35 -0700

Let's pretend to be a smart password cracker who has heard of "doing things in parallel" and design a system that would allow us to crack passwords on many machines simultaneously. One might conceive of a RPC service that accepts

incoming requests for (user-name, plain text password) pairs and tests the validity of said pair against that system's password file. One would run this service on every workstation, and obtain parallelism by making requests to all workstations virtually simultaneously.

Example:

Let's say we have a typical office environment of a few file servers with 30 workstations. We are security conscious, so we enable SUN's C2 security package. Typically, these workstations would share the same password file using SUN's Yellow Pages. All we need to do now is to install the above mentioned service on all of these workstations and we can check about 30 passwords in parallel. Not bad, if we could just find a way to get that service running on all workstations...

Gee... I wonder what rpc.pwdauthd does? Bingo! Here is EXACTLY the desired service. It already runs on every SUN with C2 enabled!

When C2 is enabled, the password part of the password file is hidden from users. Rpc.pwdauthd fills the gap by providing a service whereby a (user-name, plain text passwd) may be verified; this service runs on every workstation. One makes RPC calls to the daemon to verify a password.

Unfortunately, any one from any where may do this at any time, thus leaving the doors open for distributed password cracking. The cracker doesn't have to provide his own CPUs -- he can just use all the CPUs that are in your domain!

To make matters worse, rpc.pwdauthd does NOT generate any audit records even though it makes the appropriate calls. This is a bug -- the code neglects to set the process audit-uid and audit-state, so all auditing is ignored.

Conclusion:

In order to hide passwords from crackers, we have instead offered crackers the IDEAL means to do what they wanted to do in the first place: Crack YOUR passwords, using YOUR machines, possibly using ALL your workstations!!!

00c - Caveh Jalali

Another risk of phone systems

<[anonymous]> Fri, 14 Sep 90 20:52:26 EDT

Harvard has just finished installing (at some expense) a new phone system for undergraduate use. By various threats and persuasion, HU has set up this system so that no sensible undergraduate would buy phone service from any other vendor (Only HU subscribers get listed in Harvard's Centrex directory, get Centrex service, etc.) To handle long distance (which subscribers to HU's local service automatically buy from HU as well) they have set up a Personal Authorization Code (PAC) system; to make a long-distance call from any 493-(student) phone, the caller must enter a five-digit code that is assigned at the beginning of the year. Students cannot change their codes except by going to the phone people and asking for a new one, which costs money.

A conversation I have heard at *least* five times since my arrival two days ago:

"Gee, there are 100,000 possible PAC codes, 00000-999999. And there are 6400 undergraduates [essentially all of whom live in dorms and subscribe to Harvard's phone service]. That makes a 1/16 chance that a randomly chosen code is a valid PAC code."

"So, choosing about [fiddles with calculator] 10 or 11 codes at random gives a 50% chance of hitting a valid one."

The RISK is obvious. This is obviously a frequent thread, but if an institution with so many intelligent people (like, in the CS department or Math department) can be so STUPID...

PS. My friends at MIT tell me that their system is similar. Is every college this asinine, or only the decent ones? ;-)

✓ Desktop Publishing Fraud

Sanford Sherizen <0003965782@mcimail.com> Sat, 15 Sep 90 16:09 EST

I would like to know if anyone has any experiences with, citations,and/or thoughts about DTP fraud. With a relatively low investment in scanning devices, a person could easily use desktop publishing for copying checks, certificates of deposits, currency, diplomas, grade transcripts, licenses, etc. A few cases have already been found and a relatively recent article in FORBES spelled out the problem in some clear detail.

Here are some questions that come to mind about the risks. Comments welcomed.

- * Is this truly a problem today or in the near future?
- * Are there techniques to detect scanned versus original documents?
- * Are there sufficient restrictions over the types of specialized paper stock that is used for currency and other financial instruments?
- * What are some of the developments in desktop publishing (or other related technologies) that may worsen (or even possibly contain) this type of copying?
- * What are some of the other types of documents that people have or might copy for illicit purposes?
- * If there is the capability to scan and/or manipulate financial instruments, what will happen to the national economies of nations that are (somewhat) dependent upon restricted opportunities to counterfeit these instruments?

Need some extra money? Warm up that copying machine.

Sandy Sanford Sherizen, Natick, MA 01760 USA PHONE (508) 655-9888, FAX 508-879-0698, MCI MAIL: SSHERIZEN (396-5782)

Mata cowboys and database abuse - applicant screening

Rodney Hoffman &offman.El_Segundo@Xerox.com> 17 Sep 90 07:58:18 PDT (Monday)

'Business Week', September 24, 1990, carries a story by Jeffrey Rothfeder detailing not only the all-too-common tales of mistaken identity in personal data, but a new category of "data cowboy" selling data it is illegal for employers to have:

LOOKING FOR A JOB? YOU MAY BE OUT BEFORE YOU GO IN Background checks are nosier now, and harder to fix when wrong

The lead-in tells of James Russell Wiggins being fired after six weeks on a new job when a background check turned up a drug conviction. "It turned out that Equifax Services Inc., the company that investigated Wiggins' past, had goofed: It pulled the criminal record of James RAY Wiggins. Wiggins was the accidental victim of increasingly common practice -- combing data bases to find information on job applicants....."

"Providing employee data to companies ... is a booming business, say data vendors. Sales of pre-employment data are growing as much as 75% a year for some suppliers. The larger players -- Equifax, Fidelifacts Metropolitan New York, and Apscreen, among others -- provide more than raw data. They mix information from various data bases and produce summaries that describe the applicant's financial condition, criminal and driving records, and business relationships. Despite the occasional mix-up, the big data companies have earned a reputation for thoroughness."

Such checks can cost as little as \$100, but some employers with high turnover find even that too much, and turn to cut-rate data sellers who "assemble raw, unchecked data from creidit bureaus, motor-vehicle departments, courthouses, and other sources. Problem is, some of the information may not be legal to use when hiring. 'These data cowboys worry me,' says Apscreen Pres. Thomas C. Lawson, who fears that a backlash against them could prompt restrictions on the sale of legitimate pre-employment information...."

"Information Resource Service Co. (IRSC) in Fullerton, Calif., for example, sells lists of arrests that ended in acquittal, discharge, and no disposition...." It's illegal for a employers to have such information. Other data bases, such as Employers Information Services Inc. (EIS) in Gretna, La., track employees who have filed for workers' compensation.

"Ernest Trent, a Pennzoil Co. roustabout who has 15 years experience, ripped his right arm on an oil rig in 1986 and collected workers'

compensation. Since then, he has been turned down for nearly 200 jobs. 'I'm blacklisted.'" If so, it's illegal. "Both EIS and IRSC say they can't control how their clients use the information they buy."

Inside risks of INSIDE RISKS

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 18 Sep 1990 8:31:52 PDT

My piece in the September CACM (in the inside back cover section called INSIDE RISKS) has a really strange error, in which a bulleted item appears near the top of the last column, instead of at the beginning of the conclusions section, with the other bulleted items. Constantly having to live with flaky networking, I am not surprised by anything, but do not recall having an EMail message arrive with the order of paragraphs scrambled. (We have of course had numerous reports of compression algorithms going astray, lost messages, duplicate messages, etc.) In this case, BITNET could be the culprit, because my copy of the same message was fine. A context editor problem might also be suggested.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Perry Morrison MATH <pmorriso@gara.une.oz.au> 15 Sep 90 07:30:18 GMT

Many thanks to all those who have contributed their views on issues raised in my article with Tom Forester -"Software Unreliability and Social Vulnerability", Futures, June 1990. I don't have time or space to respond in detail to all of the comments made, but I would like to pick up on some of the main threads while they are still salient for most risks readers.

First, I was never completely happy with the blanket conclusion of removing digital systems from life-critical applications, but it has served a purpose in bringing software unreliability to the attention of the general public in a fashion that has more rigour than the tabloids would provide (I hope!). In the process, it has brought what I believe are increasingly important issues back to the arena of software/systems specialists.

Although the paper restricts itself to software/hardware failures, it is highly influenced by Charles Perrow and the "Normal Accidents" argument of complex systems. As others have already stated, the central issue is really system complexity -- the limits it places upon our capacity to predict system behaviour. Unfortunately, digital systems have two other properties that exacerbate their unreliability: (a) it is easier to build much more complex digital systems than analogue ones (or at least we have so far) and (b) digital representation and computation provides more scope for catastrophic/unpredictable behaviour than analogue techniques -- essentially the "untestable number of system states" and "each state is a possible catastrophic discontinuity" arguments that we have (hopefully correctly) borrowed from Dave Parnas and others.

Our motivation stemmed from our concern that we (others, I mean) have already built systems of such complexity that we no longer understand or can predict in any adequate sense, their full range of possible behaviours. This concern is exacerbated by the tendency of complex systems to also control complex responsibilities or awesome energies and involve huge monetary investment. Such systems -- things like the Shuttle, some particle accelerator/conglomerates and others exhibit very high levels of unreliability. Note however that it is not only the digital components of such "hybrid" systems that are unreliable, but their analogue components as well -- valves etc. Again, it is enormous complexity and our inability to get adequate intellectual handles on it that is the root problem.

However, for better or worse, society is steaming down the road toward greater application of complex digital techniques... to everything -- financial systems, control of basic services, defence, communications.... In our view, this will lead to more complex digital systems with concomitant levels of unreliability and sometimes quite disastrous results. Our major purpose was to point out that in creating such powerful systems we cannot have our cake and eat it too -- we should not be surprised that when they fail (as they occasionally will being human created artifacts) the consequences will be catastrophic. The unreliability of complex systems (which, as outlined above tend to be digital) and the power/energies bound up within them should lead us to expect such consequences. Whether this scenario is any better than other alternatives (whatever they are) is a value judgement of some complexity itself. It is a value judgement because it relies upon subjective assessment of what constitutes an acceptable level of risk for a given system and the responsibilities it is tasked with.

Note also, that we tend to ignore the notion that there is more than one legitimate assessor of risk -- not just the developer or client, but the users and those that the system affects in direct or indirect ways. This is essentially the PR problem that nuclear reactors and fly-by wire systems have -- perhaps the psychological processes of individuals are often awry, but they clearly assess the risks of FBW (and the owners/operators merely mirror the commercial consequences of this concern) as worrying. In this sense, successful design is as much an educational/consultative process as abstract discussions about reliability.

I need to take some time to address the issue of risk in a way that I don't believe any commentator has to this point.

1. It is important to note that most commentators in this discussion have assumed that most system design/implementation happens in a relatively controlled, client-expert relationship where the expert has a fair degree of control over the qualities that the system will have. Often this is not the case -- increasingly, subsystems are being designed and plugged into ad-hoc mega-systems (like the international financial system communications networks) thereby adding to overall complexity without the advantage of any over-riding design to guide the development of the subsystem (apart from protocols say). I believe that this is a dangerous trend and it is a characteristic that many communications nets and other systems have -- they just grow like topsy and "design" if it can be called that is blatantly ad-hoc. Clearly, even conventional systems are added to and expanded throughout their useful lifetime, but generally some design documents are available and eventual limits to the system can be reliably assessed. Assessment of risks in the former situation and judgements of required levels of reliability can become very difficult indeed.

2. The application or nonapplication of digital techniques and the subissue of whether analogue systems are better in some applications need to be considered against some systemic cost/benefit analysis or analysis of risk (how appropriate!). Phil Maker of the Northern Territory Uni called and pointed out to me that he designed defibrillators (things that restablish the normal electrical activity of the heart I believe) and that the chances of such people dying without a defibrillator is 50% in any given year.

Clearly, software unreliability is an insignificant risk in that situation -small numbers of people with high existing risk and enormous potential benefits -- using systems of comparatively low complexity. On the other hand, a complex digital system controlling a nuclear reactor may (possibly) provide efficiency benefits that are insignificant compared to the consequences of a nuclear accident stemming from software unreliability . i.e. a situation in which marginal benefits and high complexity exist, coupled with catastrophic consequences in the (perhaps low probability) event of systemic complexity bringing about an accident.

Perhaps a less complex analogue system could be applied in this case, if at all possible. Note however that reduction of complexity in a situation with high background risk and/or potential catastrophic consequences (subjective I know) is what I would (now) advocate. (Note that the example of a computer based intensive care unit has all the qualities of a good application of complex systems -- high existing risk, good potential benefits, localised failure consequences). It just so happens (I believe) that analogue systems by their nature, limit how complex a system can become. On this point, shortly after the article was published, we received a call from someone in authority at the Shell oil company. They mentioned that they were investigating the possibility of going back to analogue systems for their drilling rigs because of their concerns relating to software unreliability.

3. In answer to the implicit question -- "what else can we do but apply digital systems to life-critical (or potentially catastrophic) situations" one should be clear that many "needs" or areas of application are only driven by the possibilities that computers provide. They are often not genuine, pre-existing needs. For example, my father hardly knew what cheques were for until later in life. Only rich people had a need for such things and banks wouldn't wear the manual processing costs for large numbers of cheque accounts. Computers eventually allowed that to happen but I'm not sure that there was a screaming demand for cheque books at the time. Yes it's

convenient and yes the whole electronic funds basis of our economies allows us to do wonderful things with enormous ease. At the same time it has created a system that is subject to massive, international abuse, theft, fraud and (perhaps) great risk of rapid systemic collapse given a sufficiently powerful event. Given these benefits and arguably large risks, is the electronic financial system a good idea? The major point however is that NO-ONE ever had the chance to evaluate the risks involved because the system grew incrementally without any central design base. It just happened.

Some of us may ask -- "how else could the international financial system be controlled?" Clearly, it can't be controlled by anything but digital techniques, since they spawned it in the first place, but the point is we know have a whole new class of problems to deal with due to the develoment of the system. This may all sound like old hat and recycled luddism, but as our article pointed out, there's no substitute for technologists being concerned about the implications of the systems they design and implement. For example, I imagine that antarctic mining would create some really interesting temperature/electromagnetic reliability problems for software and hardware designers. But for my money, antarctic mining is irresponsible with large potential for dramatic environmental damage. Obviously, we shouldn't restrict ourselves to the mere technical problems involved in our work. It might sound quaint, but too many systems are simply technology driven rather than need driven. Stop the clock, go back to the caves you ask? No, but we shouldn't complain when complexity makes unreliability a problem for implementors and an issue for the general public. If we actually EXPLAINED to the public the design contraints we face and INVOLVE them in the design, they may come to accept levels of unreliability that we think they won't tolerate. On the other hand they might throw up their hands and say "what the hell do think you're doing". Either way it would be very interesting.

4. Where does this leave us? Merely with the ideology that lots of technology commentators have peddled for a long time -- the notion that technologists must properly evaluate the implications of what they do and actively involve in the design process the people they affect. This includes amongst other things a consensus of opinion on what is a sufficient level of reliability given the array of risks. Too often we want prefabricated solutions/methodologies like "what are the best methods for providing an error minimized system at minimal cost for applications of type x". That is the engineer talking to his colleagues and designing for an abstract user group or (real) corporate owner. It is meaningless unless the designer/implementor understands that such prescriptions must be modified in the face of existing circumstances. Those circumstances include what the users and others affected by the system think.

In this same vein, some commentators seem to believe that we are hostile to probabilistic measures of software reliablity/quality. This is not so -- just that probabilities by themselves are not enough. They are meaningless without some understanding of the reliability/quality required in the intended application by the intended users. That is, as already explained, low levels of reliability may be an unacceptable source of risk in some situations (reactors?) but not in others (defibrillators) even when the software has equivalent probability of failure. How do you know how reliable the software

must be? How do we know if digital systems are best or analogue? The answer is that as a generalization, law or principle we probably don't. But in the end we should remember that we are designing for people and if they are included and fully informed and satisfied with the safety/reliability/performance provisions in a design, then that should be enough.

As always, the customer is always right.

Perry Morrison

DTI/SERC Safety Critical Systems Research Programme

Brian Randell &rian.Randell@newcastle.ac.uk> Mon, 17 Sep 90 9:38:19 BST

The following article is reprinted in its entirety from the British Computer Society's Computer Bulletin (vol. 2, part 7, Sept. 1990, p.2). It marks the launching of a new joint initiative by the Department of Trade and Industry and the Science and Engineering Research Council, to fund industry/university collaborative research projects relating to safety-critical systems. I personally very much like the tone of the article - and hope that it can be matched by the research projects that get selected. Brian Randell

```
Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK
EMAIL = Brian.Randell@newcastle.ac.uk
PHONE = +44 91 222 7923 FAX = +44 91 222 8232
```

: Safety Critical Systems - Bob Malcolm

:

: On the stairs and landing of my cottage I have four light-bulbs. A few : weeks ago the landing went dark. No, it was not a blown fuse, but the : fourth light bulb gone. As technical co-ordinator for the DTI-SERC : Safety Critical Systems Research Programme I smiled - wanly, as they : say. : : I had failed to replace the three bulbs which had failed previously. I : had fallen prey to one of the classic safety critical system problems : - failure to maintain redundant channels. Why did I do it? Why do : people store rubbish in fire-escapes? It is no good saying that 'They : shouldn't do it'. They do. What are designers to do about it? : : The challenge in building safety critical systems is to achieve safety : in the real world. We may not understand the world and may not be able : to describe it properly, populated as it is by real and really : perverse people - designers and managers as well as users and vandals. : : It is not enough to think only of 'meeting a specification', : especially when the majority of failures arise because of : specification errors. Nor is it sufficient to add something about : getting the specification right, since we can never be sure that we

: have succeeded.

: : One view of safety critical systems is that all failures have their : origins in human error of some kind - whether a design or operational : mistake, a failure to understand either a system or its failure modes, : or a failure at a higher level to appreciate and accommodate the : likelyhood of these errors. : : To produce safety arguments for systems based on reasoning about a : wide range of technological and human factors requires not only that : we compare chalk and cheese, but that we add it together in some way. : We will need to balance arguments about the style of design with : arguments about its correct construction; arguments about proof with : arguments about likelihood; arguments about comprehension with : arguments about rigorous notation. Who knows - maybe if we succeed in : general then we will succeed in the particular of reconciling : formalists and 'the rest'. To do that we would also need to make : explicit the rigour which is presently only implicit in so-called : 'informal' methods and tools. : : I doubt whether we can do all these things without the help of : psychologists, operational researchers, even philosophers. Computer : technologists and experts in application domains must work with them : to devise better global solutions and, as far as is possible and : sensible, common solutions. We must avoid the 'displacement' problem : where fixing one problem simply creates a different and perhaps worse : problem elsewhere. And we must find ways of quantifying the : effectiveness of what we do - whether as a contribution to a 'safety : argument' or to a probabilistic risk prediction. : : But we need the cooperation of all these different disciplines not : just for the particular skills which they individually bring to the : party. We need them because of their very diversity - to enrich our : intellectual stock. : : In the new DTI-SERC programme we must produce results which will be of : commercial value in the medium term. To do this we must have a firmer, : better-reasoned, basis for what we do. We might stand a chance if we : are prepared to open our minds. : : Hard scientists must stop treating soft science as non-science: soft : scientists must not feel disenfranchised. Formalists must seek the : value of what they call informal, and help in its formalisation; : informalists must find the justification for what they do. : : Safety critical systems pose problems which push us toward : co-operation between disciplines. I hope that industry and academia : seize the opportunity to do this within the new programme. :

- : [Bob Malcolm is an independent consultant in the field of systems and
- : software engineering. He currently holds a number of contracts for
- : consultancy in research and technology transfer, and is technical
- : co-ordinator for the new DTI-SERC Safety Critical Systems Research
- : Programme. He is a visiting professor at City University, London. BR]

✓ Canadian Transportation Accident Investigation

&rian_Fultz@carleton.ca> Sat, 15 Sep 90 07:31:35 EDT

The above body in Canada is responsibility for making reports on "accidents" and "aviation occurrences". They produce reports on safety related problems. With reference to report 87-A74947 "Risk of collision between Delta Air Lines Lockheed L-1011 N1739D and Contential Air Lines Boeing 747-200 N608PE <location> North Atlantic 52 degrees 14 north, 34 degrees, 00 West Long &ime> 08 July 1987.

As the report is over 4 pages long in reduced for I will give only the parts I think are risk-relevant. At 30 degrees West Longitude Delta 37 began deviating to the south of it's assigned track and closed laterally with Contential untill the aircraft crossed the assigned track of the Contential ... The front half of Deltaa 37 passed beneath the rear fueselage of the Contential 25 with less than 100 feet of vertical separation. Neither crew saw the other aircraft in time to take evasive action. The Captain used the Flight Management System to ... Passed possition report at 30 degrees west < wrong by 16 minutes > ... Gross navigaional error < deff'n more than 25 miles off > Conclusions < I am going to use the numbering of CTAT > 1) The near collision resulted from a INS < interial navigation system> data input error by the Deltal Flight 37 crew. 9) Although cross checks were contained in explicit detail in the manual used by the crew, they were set out in such terms and format that a manditory requirement to cross check at each and every waypoint may not have been clearly conveyed to aircrew. 13)The estimate for Delta 37 at 40 west showing a difference of 16 minutes was not challenged by ATC nor was it required to be... 19 no evidence was found that would indicate the Delta 37 INS was malfunctioning prior to or during the flight.lots of recommendations to make pilots make cross checks...

Brian Fultz

Kisk of Collision

&rian_Fultz@carleton.ca> Sat, 15 Sep 90 08:12:31 EDT

Between Boeing 767 C-GPWA and Boeing 727 C-GAAY < location> Toronto < time > 18 February 1987

The board writes .. < I have taken out aviation specific terms > The Boeing 727 and the 767 were on identical tracks to Toronto. The 727 was at 29,000 feet the 767 directly overhead at 31,000 feet.... ATC cleared the 767 to 11,000 feet ... ATC 3 attempts to stop 767 ... not understood ... eventually halted 1/4 mile EAST of 727 ... evasive vectors issued by ATC ... evasive instructions turned aircraft toward each other

overlapped on the controllers radar screen. The system then repositioned the

In the Pertinent information section: Radar recordings indicated that the flight data blocks for the aircraft
display: the 767 to the WEST and the 727 to the EAST < see above > The repositioned data block display was opposite to the actual relative positions of the two aircraft.

Brian Fultz

Knight reference: 'Shapes of bugs'

Pete Mellor <pm@cs.city.ac.uk> Mon, 17 Sep 90 21:34:49 PDT

In a RISKS-10.31, I wrote:

> A serious attempt *has* been made (by John Knight - reference not to hand)
> to examine the shapes of bugs in programs, i.e. the topological properties
> of those subsets of the input space which activate program faults.
> Chaotists will be pleased to learn that they were fractal.

Several people have asked for the full reference. It is:-

 Paul E. Amman, John C. Knight: 'Data diversity: an approach to fault tolerance' Proc. FTCS, 1987, pp 122-126, 0731-3071/87/0000/0122\$01.00 (c) 1987 IEEE

The paper concerns the use of `data diversity' as a means of improving program reliability, as opposed to *design diversity*. The idea is that, since the activation of a software fault depends on a particular selection of input data, it may be possible to perturb the inputs in such a way that the output is still valid in all cases, and yet not all of the perturbed versions of the input activate the fault. A voter can then process the various outputs in a similar fashion to N-version programming.

The ability to perturb inputs in a valid way depends upon the shape and size of the `failure region'. To quote:

The `failure domain' of a program is the set set of input points which cause program failure [3]. The geometry of a failure domain, which we call a `failure region', describes the distribution of points in the failure domain and determines the effectiveness of data diversity. The fault-tolerance of a system employing data diversity depends upon the ability of the re-expression algorithm to produce data points that lie outside of a failure region, given an initial data point that lies within a failure region.

...[stuff omitted]

We have obtained two-dimensional cross sections of several failure regions for faults in programs used in a previous experiment [5]. ...[stuff omitted]

The cross sections shown are typical for these programs. This small sample illustrates two important points. First, at the resolution used in scanning, [The inputs are simulated data from radar scanners tracking an object. - PM] these particular failure regions are locally continuous. Second, since the failure regions vary greatly in size [by a factor of 4×10^{-10} ! - PM], exiting them varies greatly in difficulty.

[End quote]

You will see that the authors do not, in fact, claim that the failure regions described in this paper are fractal, so apologies if my statement misled anyone. However, they cross-refer another paper which describes these faults:

S.S. Brilliant, J.C. Knight, N.G. Leveson: `Analysis of faults in an N-version software experiment', University of Virginia Technical Report No. TR-86-20, September 1986.

The two papers cross-referred in the above extract are:

- [3] F. Cristian: 'Exception Handling', in 'Resilient Computing Systems', volume 2, T. Anderson, ed., John Wiley & Sons, New York (to appear).
- [5] J.C. Knight, N.G. Leveson: `An experimental evaluation of the assumption of independence in multiversion programming', IEEE Transactions on Software Engineering, Vol. SE-12, No. 1, January 1986, pp 96-109

BTW my mail system has been playing up. If anyone has mailed me, e.g., to request a copy of the Forester and Morrison paper, and not received a reply, please retransmit.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Applicability of software curricula

Michael J. Konopik <zzz@NISC.SRI.COM> Fri, 14 Sep 90 17:02:21 PDT

In his discussion of software certification in <u>RISKS 10.38</u>, Theodore Ts'o made a sweeping condemnation of the MIT software engineering curriculum. He argued that it sidesteps the real world by teaching "completely dated" languages and not teaching the use of any commercial SE tools in the classes. I never thought I'd stand up to defend anything about MIT; but I wanted to add some more context on the issue for those who weren't exposed to this curriculum.

It would seem that Theodore was so intent on blocking out the Liskov philosophy of programming that he didn't hear the statement of the purpose of 6.170. In fact, the same teaching strategy was applied in 6.001 and 6.004, as well. None of those classes taught their material using any "real world" languages or tools. The professors all gave pretty similar disclaimers that went something like this:

We're not here to teach you C. We're not here to teach you how to use any particular set of tools. On the contrary - our purpose is to teach you a framework of fundamental concepts. And if we use commercial tools and languages to teach it, many of you will spend too much time concentrating on those things instead of the material itself. The languages and tools we use are in themselves functionally complete. They are tailor-made to facilitate teaching the material. And when you finish the class, you will be able to apply what you learn to whatever environment in which you find yourself working, without being biased to any one specific set of languages or tools.

After the exam for 6.001 (in '82), I met Sussman on the 9th floor of NE43 to express my appreciation for the course. I told him that I had really grown to like Scheme in a big way, and I asked him if it would be possible for me to obtain updates to the language manual as it evolved in the next few years. His stern answer was "Absolutely not!" I pressed him - "Why??" His answer has stuck with me. Quote not quite exact: "You completely missed the point, Mike. Scheme was just a teaching tool. So what if you can write programs in it? After 6.001, you should be able to pick up half a language in half a week. And for almost any program you want to write after this, there will be at least three other languages out there that are more suitable for writing the program than Scheme will be. Forget the language - remember the material!"

Heck, the assembler they taught when I took 6.004 didn't even exist, except on paper!! But it still conveyed the ideas they wanted to teach pretty well.

Regarding CLU and Liskov's "religion": Theodore's assessment sounds a little bit extreme. We had the evils of globals preached to us, too. But the point was made that programmers should avoid using globals WHENEVER POSSIBLE; because for one thing, it's usually cheaper to pass around one-word pointers to large objects than to have to manage a huge heap of globals. We were also force-fed the top-down programming methodology. But one of our lectures had a mention of how it usually works in the "real world", calling it something like the Iterative Method (design - code - test - loop). The "One True Way" was just the idealized classroom method. Maybe they don't discuss that anymore, or maybe Theodore punted that particular lecture...

To make a short story long - sure, they didn't teach a lot of reality in MIT's SE curriculum. But in my opinion, what they did teach was of much greater long-term value. For the concepts being taught apply to more than just the software development environment that is preferred at the time. Teaching everything with "current" models runs a risk of rapid obsolescence.

-Mike

M The need for software certification

Joe Marshall <jrm@lucid.com> Sat, 15 Sep 90 10:26:13 PDT

I am against certifying software professionals. I agree with Mr. Ts'o that professional certification would lead to a "guild". Like Mr. Ts'o, I think that my style of programming is near perfect and I always write nearly bug-free code. Like Mr. Ts'o, I am afraid that I would be excluded from the "in-group" for reasons that have little to do with my outstanding ability to write bug-free code on the first pass with no expressed design goals.

But before we start excluding undesirables from our midst, we should look at

what we are trying to accomplish. I think most of us would agree that we want to have computer systems that reliably accomplish their stated purpose (leaving aside the ethical questions of what purposes are worthy). In order to scientifically engineer such systems, we need a way to measure the reliability. This would include examining failure modes, assigning probabilities to them, and evaluating the undesirability of such failures.

To some extent, this is a black art in the realm of software engineering. I know that I haven't been trained in this. If we could devise some measure of reliability of software, then we could easily determine which design methodologies are best suited to producing reliable software. Then, any person who could not or would not follow these methodologies would find it difficult to make a career in software engineering.

The CLU group at MIT made a concerted effort to address some of the issues of software reliability. While many people found the "religious" atmosphere of the class repressive, I think the basic principles behind the religion have merit and cannot be dismissed as "dated" or "archaic". It was developed in the 70's, long after teletypes and punch cards. "Modern" languages (C++) and "modern" operating systems (Unix) have yet to address the goals of such "arcane" languages such as CLU and ALGOL and "arcane" systems such as Multics.

I understand that MIT does not offer an accredited computer science program.

~JRM

Software Workers Guild/Union

Jerry Glomph Black <black@ll-null.ll.mit.edu> Sat, 15 Sep 90 10:43:48 EDT

>I am against the "certifying" of software professionals. ...

I fully agree, all we need is another champion of excellence rivalling the public teachers' unions. One of the last bastions of intellectual and economic freedom & independence is in the software industry & craft. Trash this enterprise as well, and we all might as well start cracking open our 'Dick & Jane' Japanese primers. Now I know why so many computer nerds espouse Libertarian dogma, it is their appreciation of their relative intellectual & economic freedom compared to most stifled workers. In most endeavours, creativity, originality, and excellence is stomped on by some actual or de-facto regulatory or union body. TYTSO's description of the Software Engineering course at MIT sounds like another tentacle of the octopus. Global variables are anathema? How about pointers to data structures?

Jerry Glomph Black, black@MICRO.LL.MIT.EDU (Independent software guy)

Ke: The need for software certification

Martyn Thomas <mct@praxis.co.uk> 17 Sep 90 14:02:54 GMT

In RISKS 10:38, Theodore Ts'o gives many reasons why he believes that ceryifying software professionals is a bad idea.

Certification undoubtedly brings problems - but so does absence of certification. The criticisms he makes would apply, mutatis mutandis, to certifying medical practitioners and lawyers, yet many societies have decided that such certification is desirable.

On balance, I believe that some limited certification is desirable, for staff who hold key positions of responsibility on projects which have significance for society. (This is an imprecise phrase, which is intended to include safety-critical systems, systems involving national security, systems involving substantial sums of public money, and so on. I have no doubt that an adequate mechanism for defining such projects could be devised). Many countries (including the UK) already have such mandatory certification for other engineers.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

Ke: The need for software certification

Phil Windley <windley@ted.mrc.uidaho.edu> Mon, 17 Sep 90 10:27:22 PDT

Theodore Ts'o <tytso@ATHENA.MIT.EDU> makes several objections to certifying software professionals: [...]

Couldn't these same objections be made to professional certification in other engineering disciplines?

I will grant that what constitutes "good engineering practice" is much better defined in mechanical engineering than it is in software engineering and thus it might be easier to develop a test for mechanical engineering competency than it is for software engineering. What is the history of this? Does anyone know when the first professional engineering certifications were done and what kind of trouble this caused for the discipline trying to figure out what to put in the test?

Even so, having to come up with such a test would certainly create a lot of discussion, much of it worthwhile.

The second point is, I think, more easily dealt with. I don't think that professional certification has led to a "unionization" of engineering. And certainly no one would contend that the fact the a person is certified means that their designs are error free. So why would this occur for software engineers?

Most engineering activities that affect public safety (in areas where

certification is done) must (by law) be reviewed and approved by a certified engineer. This approval say, in effect, "This design conforms to good engineering practice for my field."

Has anyone on the list been involved in a large software project that affected public safety where such a review was or was not done (and will they admit it ;-).

Phil Windley, Department of Computer Sciencem University of Idaho, Moscow, ID 83843, Phone: (208) 885-6501

RE: The Need for Software Certification

<fostel@eos.ncsu.edu> Mon, 17 Sep 90 15:19:38 EDT

As an old alum of both the MIT undergrad computer science program and an early version of Liskov's software engineering course, my eye's perked up when I saw Ts'o rip it assunder in the course of analyzing the need for "software certification". I also teach an undergrad course on software engineering here at NCSU, and perhaps that somewhat colors my perspective.

Although the title of the post by Ts'o was "software certification" the subject matter seemed to be more focused on "programmer certification". While I share much of the trepidation that motivates Ts'o, my concerns are somewhat different. An analogy might help. In the construction industry, there are a number of different classifications of individuals by their training, function, experience and so on. Two that are well understood are "architect" and "master carpenter". To some degree, an architect can generally do many of the things a master carpenter can do, and vice versa, and to some degree, each probably thinks that their own slant on the problems of construction cuts to the core of the "real" problems in construction.

But, is the distinction between the two one which is unwise and a danger to the building industry and more generally to society at large? Clearly No. It may, however, be a danger to a skilled carpenter who wishes to move into the domain typically populated by architects. Even though that carpenter may in fact have talent and experience which is superior to many architects, it is not in the interest of society to freely allow such fluidity in job descriptions and job certifications. Conversely, the architect may find their actions on a job site to be limited by lack of certification as a carpenter. (My brother is an architect and this is a very frustrating problem for him at times.)

The reason for the limitation of the roles of the architect and the carpenter is the underlying assumption that without an individual going thru a certain process of training and examination, that individual can not quite be trusted to perform certain actions that could bring risk to the public as a result of an error made in that capacity.

Precisely the same sorts of reasons can be used to justify the existence of certified skills within the domain of software engineering, and no doubt it is only a matter of time until this is done. Ts'o is concerned that this will

lead to a limitation of an individuals ability to work on certain projects and of course this is precisely the intent.

Perhaps Ts'o would be more content with this arrangement if the prevailing trend in software engineering were towards the flamboyant and powerful style of development at which he is no doubt quite expert. After all, in this way he could be more confident that the software controlling the 747 he flew in or the nuclear powerplant he lived near, was not built in a plodding fashion by people who believed in flowcharts and pseudo-code, or by people who bothered to design a system before they began to build it, or by people who had their designs validated by independent experts before wiring potentially erronious assumptions into hundreds of thousands or millions of lines of code.

I would have little fear of living in a house hammered together by my brother the architect, nor would I be concerned if Norm the carpenter (From PBS This old house series) designed the layout for my house. But I'd not set foot in a 50 story building built without consultations from CERTIFIED structural engieers, with blueprints thouroughly reviewed by CERTFIED architects, and construction performed by professional, CERTFIED contractors. The issue is scale.

I trust Ts'o or most other competant programmers to develop a simple data base program, word processor, compiler, or a host of other applications programs. (Though I might not trust them with my capital without a track record as "certified moneymakers".) But large, complex software systems have problems that are not readily visible in the small scale applications.

In my software developement courses, I commonly tell students that the methods which will be required of them are not necessarily the most efficient methods for the class project required of them. For the trivial sort of work I can require of students in a semester, there is really no need for comments since they will remember everything all the time, and there is no need for requirements analysis since they will usually be both customer and producer, and there is no need for formal design since they must begin work on the code before I have a chance to provide formal feedback on their formal design, and so on for most of the techniques of software engineering.

On the other hand, as the size of the problem grows, and the customer becomes distinct from the development, and the development staff becomes fluid, and the effort expands in numerous other dimensions towards bewildering complexity, the methods I prescribe are in fact neccesary...but that must be taken as an article of faith. There is no way for students to actually participate in a 5 year development of million line system in a few months of class time. It's unfortunate that more students, esp the bright and energentic ones like Ts'o, do not understand that. Perhaps equally, it is unfortunate that the professors, like Liskov, do not find ways to make these students understand it.

Will programmers be certified? Definitely.

How will they be certified? By the processes and standards used by the leaders of the industry when certification finally becomes inescapable.

When will certification begin? Probably shortly after a disaster involving software that was not up to snuff and was produced in questionable fashion.

Will it be a source of frustration to software developers? Of course.

Will it make the public safer? Hopefully.

Gary Fostel, Dept of Computer Science, North Carolina State University, Raleigh,NC, 27695-8206fostel@eos.ncsu.edu919-737-3195

Ke: The need for software certification

Theodore Ts'o <tytso@ATHENA.MIT.EDU> Fri, 14 Sep 90 13:56:55 -0400

>Surprisingly, version control (such as RCS) was never discussed at all.
>I suppose the theory was that if we designed everything in pseudo-code
>from scratch, we would never need to rewrite or revise any of it, so
>version control was considered important. I will leave it to the Gentle

v not

>Reader's judgement as to whether or not you can teach a reasonable>Software Engineering in today's environment, when several people can be>changing files on a networked filesystem, without at least mentioning>version control.

Err.... oops. I should have proofread this a bit better. The sentence makes a lot more sense with the negation in there..... Sorry about that!

- Ted



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter Denning <pjd@riacs.edu> Tue, 18 Sep 90 15:20:25 PDT

In <u>RISKS-10.3</u> of 13 Sept 1990 David Murphy says, "It is completely impossible to build a fair arbiter or synchroniser." He also says, "... any digital design technique is just a way of improving engineering confidence in the product, not of guaranteeing correctness." These statements are not true. I hear them repeated frequently enough that I surmise they are part of the folklore. I write here with an antidote.

First, a definition: An arbiter is a device that selects exactly one out of a set of requests represented as signals on input channels. The arbiter must work even if two or more of its inputs can change simultaneously. This behavior is considered "fair" since it does not give preference to any one input. Arbiters are used at the ports of memory modules, in the nodes of interconnection networks, and in interrupt systems. It is easy to build such circuits.

The fundamental theorem of arbiters is: There is no fixed time bound for the arbiter to make its choice. The reason is that if two inputs change simultaneously, the device can enter a metastable state from which it will exit after a random amount of time (to be precise, the probability that the circuit persists in the metastable state for more than t seconds is exp(-t/A), where A is the mean switching time of the circuit). If we as RISKS readers demand that every arbitration be performed correctly, we must use asynchronous circuits that will wait until an arbiter has settled. These circuits are provably free of synchronization errors.

But if we build an arbiter into a computer that assumes a fixed time for an arbiter to reach every decision, there is a chance that the arbiter will not be settled down and the half-signals at the arbiter's output may cause a malfunction in the rest of the computer. Although the probability of this failure might seem small, failures every few days become very likely at the clock speeds of modern computers. If you are interested in reading more about this, you can take a look at my American Scientist article (1985) and also Chuck Seitz's chapter in the Mead and Conway book (1980).

Another common misunderstanding about arbitration concerns the lowest level at which an indivisible operation must be implemented. Dijkstra's solution to a concurrent programming problem (1965) was a software arbiter that relied on the existence of arbitration in the memory addressing circuits for individual memory locations. Lamport showed how to achieve fair mutual exclusion without any requirement that references to memory cells are arbitrated (1974).

Conclusion: we know how to build fair arbiters and how to design circuits that are free of synchronization errors.

READINGS

C. L. Seitz, Chapter 7, "System Timing," in Introduction to VLSI Systems, by C. Mead and L. Conway, Addison-Wesley, 1980.

P. J. Denning, "The Arbitration Problem", American Scientist (Nov-Dec 1985).

L. Lamport, "A new solution of Dijkstra's concurrent programming problem", Communications of ACM (August 1974), 453-455.

Ke: Security compromise with SUN's C2 package (Jalali, <u>Risks-10.39</u>)

Li Gong <li@diomedes.UUCP> Tue, 18 Sep 90 17:24:03 EDT A related point: the C2 design still allows an intruder to guess user passwords even if rpc.pwdauthd is not present. Everyone has a pair of public keys for authentication, RPC, and the like (public key K+ and corresponding secret key K-). In file /etc/publickey which is readable to anybody, there stored (among other things)

[user_name, K+, E(p, K-)]

where E(p, K-) is K- encrypted with key p (generated from user password) under DES. An intruder can download this file, guess a p' and decrypt the last item with it to get a K-'. Then he can choose any text X and verify D(K-', E(K+, X)) = X, where D is decryption. If the above holds, he is quite certain that p' is the correct password.

This kind of attack is called Verifiable-Text Attacks (see my paper in Proceedings of Infocom '90, June). It can be conducted off-line, then you have to use your own CPU of course.

Li GONG, Odyssey Research Associates, Inc.

Ke: Expert system in the loop (Philipson, <u>RISKS-10.38</u>)

<henry@zoo.toronto.edu> Wed, 19 Sep 90 13:44:13 EDT

>In the case of the Vincennes, it cannot be disputed that a mistake >was made. The Pentagon found no human responsible for it, so it >must have been a mechanical error...

I fear Clifford is departing a bit from his usual standards of objectivity and precision, here, and the distinctions are important. Was a mistake made? Clearly, yes, since there was no need to shoot down a civilian airliner. Was it a *preventable* mistake? Now this is a harder question, as is the question of who should have been responsible for preventing it. (My vote goes to the airline and/or pilot who decided to fly an airliner through a combat zone.) If I'm not mistaken, the Pentagon's finding was not that nobody was responsible for the mistake, but that no *blame* was attached to the captain and crew as a result of it, i.e. their decision was reasonable in the circumstances and no disciplinary action was in order. Whether or not this finding was correct, the general point stands: one should beware of the assumption that there *must* be a villain, that either some human must be guilty or there must have been a mechanical failure.

The Vincennes disaster could have been averted if the airliner had followed a safer route, if the Vincennes had not been in combat (and hence inclined to treat potential threats as real ones) at the time, if the captain and crew had been trained to be more skeptical of the computerized reports and more thorough about cross-checking them, or if the equipment and software had been better designed. Which of these is the villain?

(Actually, I agree with Clifford's main point, that meaningful human decision-making requires sufficient time and adequate independent sources of

information. It's not clear to me that the Vincennes case is a good example of total lack of same, however, so much as a case of how conflicting or doubt-casting evidence gets ignored in a crisis.)

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

Re: Expert system in the loop (Philipson, <u>RISKS-10.38</u>)

<henry@zoo.toronto.edu> Wed, 19 Sep 90 14:10:23 EDT

>... Military personnel have, by joining or
>accepting induction into armed service, accepted certain risks.
>Civilians have not. If there is any doubt whatsoever that the
>approaching plane was hostile, the Captain should have decided not to
>destroy it, accepting the risk of outcome #3, i.e., that his ship might
>come under attack ... He and his crew signed up for that risk...

One should remember that soldiers are not policemen. Policemen generally are required to accept risks themselves rather than passing them on to civilians; their *job* is reducing civilian risks. The military are not in quite the same situation. Their job is to carry out the policies of their government, and if innocent people get hurt, that is the policy-makers' problem. Military actions often involve injury or death to innocent civilians, and avoiding this entirely is probably impossible, although minimizing it is usually desirable. The captain and crew of the Vincennes signed up to risk their lives in protecting the United States (and its allies and interests), not in protecting civilians in general.

>... The passengers of the airliner had accepted no such risk...

Their government had accepted it on their behalf, by initiating warfare against foreign vessels, for what it presumably considered adequate reason. Governments in general feel that they have a right to risk the lives of their citizens -- without their individual consent -- for sufficient cause.

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

expert systems in battle (Cliff Johnson, <u>RISKS-10.39</u>)

Steven Philipson <stevenp@decwrl.dec.com> Wed, 19 Sep 90 15:43:55 -0700

In <u>RISKS-10.39</u> "Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> writes a response to my post on expert systems.

First, I request that more care be exercised in the use of quotations. The excerpt that Clifford used appears to be attributed to me (through the use of a single greater-than sign) when the excerpt was one that I was quoting from someone else. The usage in this article will be a ">" in the first column to denote quoted material.

>In the case of the Vincennes, it cannot be disputed that a mistake >was made. The Pentagon found no human responsible for it, so it >must have been a mechanical error.

This statement is in error. Please, READ THE REPORT. Human error on the part of two officers was specifically cited, and inadequacies with the systems were noted. An error was made by a junior officer in reading both the altitude and speed of the approaching aircraft. Error was also attributed to a senior officer for not confirming the data on his own by checking his own displays. The board also found that inadequacies in the design of the display increased the probability for misinterpretation of data under the stress of battle. The board found that Captain Rogers made a correct decision to fire based on the data that he had available to him.

>The assertion that humans have

>time to meaningfully evaluate the computers' information in a few >minutes is patent nonsense (as proven by the Vincennes)

I never made that assertion, nor do I hold that it can be done. In my previous post I wrote "All this may not be possible to do in practice". Indeed, it is not reasonable to expect that large bodies of data and rules of reasoning can be evaluated by a human being within a few seconds. On the other hand, the raw data cannot be assessed by a human in that time frame either. Some amount of processing is going to be done by machine. A decision as to how much should be done must be made at some point. In the case of the Vincennes, only minimal processing was performed, and the radar data was presented fairly simply -- as a course and altitude readout. Even that was misinterpreted under the stress of battle.

One must also consider that not all battlefield decisions are made on a time frame of seconds or even minutes. Assessments of the enemy's intentions often occur over periods of days and weeks. An expert system that finds evidence of significant activity and reports it could be of great value to commanders if the time frame is long enough to evaluate those decisions and actions.

>- all humans can do is to *gamble* whether the computers (or their readings >of the computers' consoles) are right, and so they act as no more nor >less than randomizing agencies -

In a sense, that is correct -- they do gamble that the machines are right, but we do this every day in all forms of endeavor. When I drive my car, I gamble that my speedometer is close to correct, and that by following it I will avoid getting a speeding ticket. The gamble is a good one as I have a sense that the probability of it being correct is high, although it could be wrong (and has been on occasion). Likewise, one "gambles" on the correct performance from more complex systems, but these bets are far from random. The key point here is that a computer system does not have to be perfect to be useful, even when used in critical applications.

>Such decisionmaking is de facto *governed* by computer: without >computer prompts, no retaliatory decision at all would be taken;

Again, incorrect. Decisions to fire were made long before we had computers

-- they are not required to make these decisions. Data collected by human observers can be and is interpreted incorrectly as well. In addition, use of a computer system does not preclude the consideration of other data points. Friendly and/or non-hostile craft have been destroyed in the past in cases where there was no computer involved. By the way, the use of the word "retaliatory" is incorrect here. The decision to fire in this circumstance is not an act of revenge, but rather of self protection.

It is a hard reality that decisions must sometimes be made in the midst of chaos, with few or unreliable data points. The presence of computers does not change this. Computer systems have been involved in cases where the outcome was not as desired. There have also been many cases where similar mistakes were made without the use of computer systems. The banishment of computers from critical systems will not stop such the occurrence of such errors.

expert systems in battle (Jeff Johnson, <u>RISKS-10.39</u>)

Steven Philipson <stevenp@decwrl.dec.com> Wed, 19 Sep 90 15:43:55 -0700

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> writes:

>The captain of the Vincennes was faced with a decision that had four >possible outcomes:

- > 1. Destroy approaching plane; plane is hostile (CORRECT OUTCOME)
- > 2. Destroy approaching plane; plane is not hostile (ERRONEOUS OUTCOME)
- > 3. Don't destroy approaching plane; plane is hostile (ERRONEOUS OUTCOME)
- > 4. Don't destroy approaching plane; plane is not hostile (CORRECT
- > OUTCOME)

This is an interesting set of rules, but it does not reflect the rules that were in use in the Gulf. The above rules assume certainty in the identification of aircraft. Actual rules are based on probable identification.

This can be seen directly in the transcripts from the Vincennes, where crew members used terms such as "probable hostile" and "possible comm-air". The captain of the Vincennes had a primary responsibility to protect his ship. In this case, given a "probable hostile" aircraft on a probable attack profile, the correct decision is to fire. What's more, the destruction of a non-hostile aircraft is NOT an erroneous outcome. This isn't to say that it isn't a terrible tragedy -- it is. It is however, a correct action given the military doctrine in use.

US fighter pilots in World War II made a point of staying well clear of ALL ships (not just enemy vessels) as they were likely to be fired upon if they got too close. The pilots knew that the rule of operation for the ships was "better to shoot down a friendly aircraft in error than to lose a ship". The captain of the Vincennes was operating by the same rule. This was a major factor in his being found to have made the correct firing decision. Whether this value judgment is a good one or not is a completely different question.

- > Military personnel have, by joining or accepting induction into
- > armed service, accepted certain risks. Civilians have not. If there
- > is any doubt whatsoever that the approaching plane was hostile, the
- > Captain should have decided not to destroy it, accepting the risk of
- > outcome #3, i.e., that his ship might come under attack (Note: not
- > even necessarily that his ship or crew would sustain any injuries).

These are reasonable statements, but irrelevant. We can argue about what the rules of engagement should have been, and even whether either US warships or civilian traffic should have been there at all, but that will not change the situation that occurred nor rules that were in effect. The rules did not state "fire only if *sure* of hostile intent", but rather "US warships will fire to protect themselves if threatened". Part of the reason for this is that the US had already suffered casualties in the Gulf in the case of the Stark. The board of inquiry found that the captain acted in accordance with the rules and his orders.

I heartily recommend that all persons who are concerned with the issues of computer systems in critical applications read the Vincennes report. Many insights can be gained through examination of the performance of both humans and machines. There is much of value here for those who design systems, whether they include humans, computers, or both.

Ke: Expert system in the loop (Whose fault was the Vincennes...?)

Walt Thode <thode@nprdc.navy.mil> 20 September 1990 1316-PDT (Thursday)

There seems to be a fair amount of interest about who is to blame for the mistaken destruction by the USS Vincennes of a civilian airliner. There are various points of view.

Clifford Johnson (in <u>RISKS-10.39</u>) suggests that > (...) it cannot be disputed that a mistake > was made. The Pentagon found no human responsible for it, so it > must have been a mechanical error. (Recently, Captain Rogers was > awarded a special medal of honor for his courage in commanding the > Vincennes through the shootdown.)

I hope he meant the above with considerable tongue in cheek. Suggesting that the Pentagon's findings in a controversial case like this would be altruistic is naive at best. A possible indicator of the Pentagon's actual response is that Capt. Rogers, despite his impressive credentials up to the time of this tragedy, is now unlikely to be promoted to the Flag rank (Admiral) that was probably a foregone conclusion before this incident. (This is not necessarily a logical decision, however; the Navy tends to sidetrack any career that becomes besmirched with controversy or scandal, and the Captain is always responsible for the events in his command, even when he in fact often may have little control.)

Johnson's further comment is right on: > The assertion that humans have > time to meaningfully evaluate the computers' information in a few
> minutes is patent nonsense (as proven by the Vincennes) - all
> humans can do is to *gamble* whether the computers (or their readings
> of the computers' consoles) are right, and so they act as no more nor
> less than randomizing agencies - i.e. one would get the same level
> of "judgment" by card shuffling.

An important issue here is not mentioned. Systems are designed by people, and often people do not design man-machine interfaces very well. The interface should maximize the chances of making a good decision in a case like this, and should minimize the chances of making a bad one. It's often the case that systems are designed, developed, and fielded with poor man-machine interfaces. (I don't have extensive knowledge of the AEGIS or other Vincennes systems, so I'm not in a position to judge them in particular.) I suspect that there is much to yet be learned about what comprises a good man-machine interface in instances like this one.

--Walt Thode thode@nprdc.navy.mil {everywhere_else}!ucsd!nprdc!thode

Kailway Safe Working - large analogue systems (skill, <u>RISKS-10.36</u>)

Peter Jones <AINT@UQAM.bitnet> Wed, 19 Sep 90 15:28:56 EDT

>outside the train (by climbing down to the trip and manually resetting it).

In the Canadian climate, this would introduce a risk of the driver slipping and falling in conditions of snow, ice or sleet. Not a procedure to be taken lightly.

>... signal box interlocks are implemented by requiring two largish pieces of
 >metal to occupy the same space for conflicting events to occur. The only
 >failure mode here is severe deformation of the metal rods.

Or a failure in the linkage to the signal.

> These drop in sequence at a rate which >reduces the train speed to around 20 km/h.

I think the elevated in Chicago has (or had in 1970) a system like this to regulate train speed at an 'S' bend around 39th South. A train would encounter a red at the the start of the 'S', which would change to yellow as the train arrived. Then, there was a series of signals that would change from red to yellow as the train proceeded slowly through the 'S'. Speed control appeared to be done manually under the driver's control.

>long distance diesels have a vigilance button which must be pressed every
>sixty seconds to keep the brakes off. It's a good thing that brakes are
>applied automatically because it is commonly believed that old hands can press
>this button even when sleeping. I've observed the automaton-like way that
>drivers press this button and I have no doubt that it happens.

In 1968, I saw a film of the SNCF (French Rail) workers explaining their dead-man system. Originally, it was a kind of steering wheel that had to be held up. When the SNCF discovered the drivers were holding it up with a piece of string, they changed the system so the driver had to raise the steering wheel every 20 seconds. Drivers found this exhausting. I'm wondering if a less obtrusive system couldn't be used. Maybe a throttle with a light feel but requiring almost continuous holding. The safety system would detect the natural "dither" of the driver's hand.

I'm also surprised at the number of cars fitted with cruise control, and NO vigilance system. Some drivers, to avoid the hassle of re-engaging the cruise control, allow themselves to almost plough into the next vehicle, rather that reduce speed slightly. Many controls will maintain the preset speed, but seem to lack a throttle-like means of reducing speed by say 5-10 kph.

>Mind you, it all seems very safe compared to Canada where express passenger >trains are managed using CTC and walkie-talkie radios. I've seen passenger

The Mulroney government seems to be using a probabilistic approach: make accidents less likely by cutting back drastically on the number of passenger trains :-)

Peter Jones UUCP: ...psuvax1!uqam.bitnet!maint (514)-987-3542

Ke: I'm 99% Sure You're A Crook!!! (mmm, <u>RISKS-10.39</u>)

The Polymath <hollombe@ttidca.tti.com> 19 Sep 90 23:43:48 GMT

}[To me, it seems like there is quite a range of quality in the machines used }to verify my credit. Some are solid-looking hardware from NCR or IBM with }expensive keyswitches and plasma displays. Others are cheapo stuff with LED }displays and calculator-style keypads. I guess PW went with the system from }Ma & Pa Kettle POS Systems. mmm]

This is more a marketing risk than a computer risk, but still something to consider. "Solid-looking hardware" with apparently expensive switches and displays may well mask shoddy hardware and software internals. I've particularly noticed this technique in electronic products from a certain Japanese manufacturer. Their smaller boom-boxes, for example, have slabs of metal bolted to the inside of the plastic chassis, apparently serving no other purpose than to give the feel of solid, heavy quality to an otherwise cheap and mediocre piece of equipment.

With the advent of systems like NeXT that make the building of impressive graphic user interfaces relatively simple, we need to learn to worry about what internal software sins those GUI's cover.

(A related risk has been around for some time: Modern word processors and printers make rough drafts look like finished products).

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

Mook suggestion: Apollo, The Race to the Moon

"Cheap, fast, good; choose two 19-Sep-1990 1004" <minow@bolt.enet.dec.com> Wed, 19 Sep 90 07:18:19 PDT

Apollo, The Race to the Moon Charles Murray & Catherine Bly Cox Simon & Shuster, ISBN 0-671-61101-1

RISKS folk will probably find this book interesting: it's a history of the Apollo project told mostly from the viewpoint of the engineers (and especially the flight controllers and back-room support staff). It is not a history of the astronauts.

There is a great deal of emphasis on safety issues, including second-by-second descriptions of some of the emergencies: the launch-pad fire, the Apollo 11 landing computer overload, the Apollo 12 lightning strike, and -- especially -- the Apollo 13 rescue.

The book is journalism, not science; so RISKS readers will have to determine for themselves how the lessons of Apollo are applicable to their work (and how many have been lost since the Apollo project).

I found a hard-bound edition in the remainder pile in a Cambridge (MA) bookstore; so you might have to dig around for it.

Martin Minow minow@bolt.enet.dec.com

Ke: Knight reference: `Shapes of bugs' (Mellor, RISK-10.40)

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Tue, 18 Sep 90 12:28:11 -0700

> However, they cross-refer another paper which describes these faults:

> S.S. Brilliant, J.C. Knight, N.G. Leveson: `Analysis of faults in

- > an N-version software experiment', University of Virginia Technical
- > Report No. TR-86-20, September 1986.

This paper appeared in IEEE Trans. on Software Engineering, February, 1990.

ACM Conference on Critical Issues in Computing

"Harold S. Stone" <STONE@IBM.COM> Wed, 19 Sep 90 09:22:13 EDT

The ACM Conference on Critical Issues (6-7 November 1990, Hyatt Regency,

Crystal City VA) is unique in the following ways:

It is a summit meeting.

The attendees will include key decision makers, IS executives, researchers, and users. AT&T, IBM, TRW, and other Fortune 500 companies will be represented.

It is devoted to two important practical issues

The critical issues are modeling reality and managing the complexity of large systems.

It is a working meeting with audience participation.

The attendees will spend one day in working together in small groups.

It will produce an action agenda.

The joint work of the audience will identify the specific problems to be attacked and who should address these problems. The output will be an agenda of actions that could help to resolve the issues raised in the years to come.

Besides the technical speakers listed on the program, there will be a keynote address by Dr. Gene Wong who is now on Allan Bromley's staff in the OSTP of the White House while on leave from UC Berkeley. I am sure that you will be interested in his comments in regard to the government's role in setting strategic directions in computing for the future. The dinner speaker will be Oliver Selfridge whose talk is entitled ``We can't go on programming like this.'' Other speakers of note on the technical program are David Parnas, Jay Forrester, and Stuart Dreyfus.

Program:

Modeling Reality Section

Speakers: Stuart Dreyfus, Jay W. Forrester, John C. Kunz, Eleanor Wynn

Panelists: Jay David Bolter, Peter Denning

Managing Complexity Section

Speakers: David Parnas, Rod Leddy, Edward Chevers

Panelists: Robert Charette, Peter G. Neumann

[Interested people should contact Fred Aronson at ACM HQ, 11 W 42, NY NY 10036, 212-869-7440, or send mail to issues@acmvm.bitnet .]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



🗡 certification

Richard Platek <richard@hector.UUCP> Wed, 19 Sep 90 11:17:22 EDT

Considering myself a moderate Libertarian, and hence sympathetic to arguments based on maximizing freedom and minimizing collectivistic coercion, I would nevertheless like to champion the cause of computer professional certification. Certification is not meant to protect us from MIT students like Mr. Ts'o. The truth of the matter is that the vast majority of people building computer based systems would never be admitted to schools anywhere as discriminating as MIT (I am MIT Class of 61, along with John Sununu, and very proud of it). People aren't allowed to drive cars on the road without being "certified" yet they are allowed to program systems whose failure could be more catastrophic than poor driving ability. Demanding proof of road worthiness of drivers and cars is not an abridgment of individual liberty; it is the entry fee for participating in a social process. I am as Libertarian as can be but I want the driver coming at me at 60 mph to be licensed and I want the person doing the air traffic controller software used to land my plane to be certified. Certification need not be s government function. The remarks that certification would lead to a guild do not sound negative to my ears. Guilds guaranteed the craftsmanship of their members. Certification needn't restrict creativity. It just shows one can pass some minimum requirements criteria. I go to homeopathic doctors who use very non-standard forms of medicine. Yet they all have been trained and certified in standard medicine. Although, I avoid standard medicine I feel more comfortable that the doctors I do go to have satisified all the requirements which the medical establishment has set for itself.

Re: The need for software certification

Paul Tomblin <pt@geovision.UUCP> Tue, 18 Sep 1990 10:25:31 -0400

Theodore Ts'o <tytso@ATHENA.MIT.EDU> writes:

>I am against the "certifying" of software professionals. My objections fall
>basically into two areas. The first is that there is no valid way to measure
>software "competence". How do you do it? There are many different software
>methodolgies out there, all with their own adherents --- trying to figure out
>which ones of them are ``correct'' usually results in a religious war.
[some very valid points about different approaches deleted]

>The second general objection that I have against the certification of >software professionals is that it might very well become a guild. In my >mind, there is great danger that once you have the people who are >``IN'', they will try to maintain a competitive advantage and keep most >other people ``OUT''. Mr. Whitehouse has already granted that a college >degree cannot be used to discriminate those who can program well against >those who do not program well...

>Worst yet, it could become like many unions today, and be used to protect >mediocrity within the group against people who are actually better qualified, >but who aren't in the appropriate magic group...

You just have to look at professional engineering practice to see that this doesn't need to happen. I was a professional engineer, but I choose to make my living in software, because I'm better at it. Engineering (especially Civil Engineering) is very similar to how I see the future of software developers certification because of the following:

- 1 Engineers are self regulating: Only a _panel_ of engineers is fit to judge if another engineer is incompetent or guilty of professional malpractice.
- 2 Engineers are by and large employees, rather than self employed like doctors or lawyers.
- 3 Engineering has scope for many different approaches to the same problem. A University of Waterloo grad will probably take a different approach to a problem than a UofToronto grad. They will both come up with valid solutions to the

problem, within the limits of human falibility.

4 A failure of an Engineering design can be life critical, but as long as you followed _any_ valid design methodology, you will probably not be guilty of malpractice in the event of a failure.

Engineering is not an exclusive domain. Anybody who passes an engineering course, works two years in the field, and passes an ethics exam can become one. If you don't take an engineering course, you can still become one after working 6 years and taking several exams. My father did it that way, so I know it's possible. You also have to get another engineer, a co worker or supervisor to co-sign your application. The purpose of all this is not to restrict membership, but just to show that you are capable of doing the work you are being certified for.

As a Professional Engineer, I was subject to the rules of the Association of Professional Engineers of Ontario (APEO), which has a Code of Ethics. I was also bound by the "Ritual of the Calling of an Engineer" (the Iron Ring). The "Ritual" has no legal status, but was created by Rudyard Kipling before there was a legal status for Engineers. Both of these were designed to stress to an Engineer his duty, but there is an important line in the Obligation, which is part of the "Ritual":

For my _assured_ failures and derelictions, I ask pardon beforehand of my betters and my equals in my calling...

So we admit that everyone fails at some time, and we aren't going to crucify you if you screw up, providing you did so honestly, and not because you were lazy or unprofessional.

Disclaimer: I don't speak for the APEO, and I'm not a member any more, so things may have changed.

Paul Tomblin, Department of Redundancy Department. nrcaer!cognos!geovision!pt or uunet!geovision!pt

Certification

John H. Whitehouse <al357@cleveland.freenet.edu> Wed, 19 Sep 90 08:03:09 -0400

This is a reply to Mr. Ts'o's posting in which he stated that he feared that professional certification might lead to development of a guild mentality in which those who are certified make the test as difficult as possible; he stated that the free market should be left to weed out incompetency.

The ICCP takes great pains to prevent development of a guild mentality. We certainly wouldn't like to see something like white Mark Twain described in his book, Life on the Mississippi; there. the riverboat pilots formed just such a guild. On the other hand, the ICCP takes great care in construction of its tests. Although the test items are written by those who currently hold

certificates, they are reviewed by a committee. The committee verifies that the item is correct, has only one clear answer and is not a "trick" question. A proportion of the item pool is retired each year and some of these new items are allowed to enter the test. The weighting of questions on a well-publicized outline is maintained to see that the distribution of items conforms with the outline in the study guide. Psychometricians evaluate each test and each item after the fact of test administration. They maintain careful surveillance over reliability, validity and difficulty level. The difficulty levels have not changed in any consistent direction since 1962. The pass ratio remains at about 30 percent.

I don't understand how Mr. Ts'o's fears development of a guild mentality when certification is and has been voluntary.

His belief that the free market should correct the problem of incompetence has not proven itself in practice. For the last nine years, I have been a CICS software diagnostician. I can say that almost every error that I have seen has been the product of an incompetent programmer. Some of these errors have cost the programmers' employers upwards of \$ 20,000 per incident. No one gets reprimanded or fired. I recently asked a classroom full of candidate instructors for a class on CICS Problem Determination methodology why so many CICS programmers are flatly incompetent. These instructors said, as if in one voice, that the problem is due to the fact that few universities teach CICS. The problem seems due to an inability to apply what people are taught in school. It is one thing to answer objective and essay questions correctly and yet another thing to apply it in practice. The free market fails in mid-range and large mainframe business environments because the managers are non-technical and we run software that people never saw in school. The demand for warm bodies exceeds the supply of capable people. Because of this, the free market cannot resolve the problem.

Mr. Ts'o's fails to see the problem. I warned of this sort of reaction in my posting a few days ago. I do not believe that this problem surfaces in academic environments and Mr. Ts'o's (at MIT, project Athena) is in just such an environment. I am more interested in seeing the reaction of business systems people to the problem which I describe. There, the managers will seldom see the problem and the better practitioners will tend to agree with my contentions.

Certification of Software Professionals

Kaminsky Alan R <ark@cs.rit.edu> Wed, 19 Sep 90 11:08:00 EDT

Should there be certification of software professionals? YES, ABSOLUTELY!

It's long past time for software development to be considered an engineering discipline, and for software developers to consider themselves engineers. I say this for two reasons: (1) Like other engineering disciplines, we now have formal and semiformal methods for carrying out all aspects of software development--specification methods, design methods, test planning methods, software reliability models. Our methods are now just as mathematically grounded as methods in other engineering disciplines. We CAN be engineers. (2) Like other engineering disciplines, we are engaged in constructing artifacts that the public use and that affect the public's safety. Other engineers design and build roads, railroads, bridges, skyscrapers, nuclear power plants, airplane fuselages. We design and build nuclear power plant controllers, airplane flight controllers, railway signaling systems, and CAD/CAM packages that other engineers use to design their artifacts. We SHOULD be engineers.

But if we are software engineers in the true sense of the term, we must expect to be treated like engineers by governments and regulatory agencies. We must undergo certification and licensing--just as civil, electrical, and other engineers take their Professional Engineering examination and get certified as a Licensed Professional Engineer, or whatever the procedure is in each state. And we must require that all software development projects be conducted, or at least thoroughly reviewed, by a Licensed Professional Software Engineer, who is permitted to certify that standard (software) engineering practices have been followed, that the artifact will perform correctly, and that the public will be safeguarded.

Should all software practitioners undergo such certification? NO!

Not everyone who graduates with a B.S. in engineering, and who is employed at a company to work on engineering projects, needs to become a Licensed Professional Engineer. So it should be with software engineering. You don't think you need or want to get licensed? Fine, don't. There'll still be plenty of software development work for you to do. You'll just always be in the position of needing a Licensed Professional Software Engineer to certify your work (once the government wakes up and starts licensing software engineers as they should, that is).

-Alan Kaminsky, Rochester Institute of Technology, Rochester, NY

Ke: The Need for Software Certification

Russell C. Sorber <sorber@motcid.UUCP> 20 Sep 90 01:50:45 GMT

- > When will certification begin? Probably shortly after a disaster involving
- > software that was not up to snuff and was produced in questionable fashion.

Voluntary certification of software professionals has been in existence for several years. The Institute for Certification of Computer Professionals (ICCP, Park Ridge, IL) receives support from the ACM, the IEEE, the DPMA, and several other international computer professional organizations. The literature of the ICCP also bears the logo of the IEEE and ACM.

The certification involves an education requirement, an experience requirement, passing a 5 hour, 5 part exam, and about \$120 dollars in testing fees. I vaguely remember a reduced fee for the unemployed but I'm not sure about that. The exam is given at several dozen international locations twice per year.

I became certified when I noticed job listings requesting CDP's. (Certified Data Processors). Some Chicago Board of Trade options traders seemed especialy interested in certification. This is understandable when you consider that large fortunes are risked based partly (or solely) on the output of the computer system.

I've also worked on projects (involving life and limb) where several key people involved should have had more training or certification, but didn't. I found this to be a very scary experience. (Scary enough so that I quit without other work lined up)! This experience convinced me that in certain cases, certification should be mandatory.

Nurses, physicians, pilots, civil engineers, (even hair stylists!), are all licensed. Wouldn't you want the electronic instrument that monitors your heart, or checks blood for Aids, or tells the pilot whether the landing gear is down, to be built by licensed or certified professionals?

I know I would.

Russ Sorber, CDPOpinions are my own.Software Contractor currently at Motorola Inc.sorber@marble%motcid

The need for certification

John H. Whitehouse <al357@cleveland.freenet.edu> Thu, 20 Sep 90 08:20:38 -0400

After reading yesterday's postings, I thought it necessary to reply to a few other concerns which I have noted running throughout the various postings concerning this subject.

There is a concern that ICCP certification assesses examinee philosophy. This is generally untrue. For the most part, the exams test definition and recognition at a very basic level. Some of the specialty exams go deeper, down to ability to use a concept, but not to the level of philosophy. It is truly amazing that only 30 % are able to pass these exams and that only serves to emphasize the severity of the ignorance problem. I wish to emphasize that philosophy is NOT tested and that the exams try very hard to avoid anything over which there may be controversy.

Second, I note that much of the opposition argument is founded upon nothing but fear. This is fear of the unknown because it is clear that those who wrote those postings were not familiar with ICCP certification. My thanks to those who have indicated that they have also seen this underlying thread. I also appreciate remarks to the effect that the opponents could make the same argument concerning CPAs, PEs and doctors.

Two other points: ethics and continuing education. These are two other properties of ICCP certification. I am aware that the professional associations have codes of ethics, but will they kick you out for violation ? The ICCP code of ethics is stricter than that of either ACM or DPMA and the ICCP has revoked six or seven certificates in its history. We are in an age of

viruses, hackers and white collar crime. I would think that prospective employers would view the ICCP ethics code in a most favorable light.

It has been said that the half life of knowledge in our field is three years. The ICCP requires 120 hours of continuing education every three years. Would anyone of sane mind oppose continuing education ? I would rather hire someone who I knew to have kept current than someone whose continuing education status was an unknown.

One added word concerning the guild mentality. Although exam questions are submitted by current certificate holders, they are reviewed by a committee to assure that there is one right answer (therefore not confusing, philosophical or controversial), then admitted to a pool of items. Each year, about 25 % of each exam is discarded and replaced with new items drawn from the pool. Psychometric statistics are reviewed for any old items which are retained. Those measures used are split-half reliability, the alpha coefficient of reliability, a discriminant index, the Flanagan, difficulty levI and actual counts of responses for each item. Ther are no trick questions. Great care is taken to stick to the outline and to specific weightings which have been established for outline subjects. The difficulty level for items which have been used before is monitored in an effort to make sure that target difficulty levels are retained from year to year. Those difficulty levels have carefully been maintained at 30 % pass.

Certification of software professionals

Frank Houston <houston@itd.nrl.navy.mil> Thu, 20 Sep 90 16:42:27 -0400

Being in the business of evaluating software systems and firms who develop software systems, I read the commentaries on certification with great interest. I have my own opinion, which I have discussed in this forum before and to which I will refer presently; but first I want to add my fuel to the flames that Mr. Ts'o ignited.

Mr. Ts'o tells us how he and a group of students got an "A" for a school project while ignoring a great many software engineering techniques. I maintain that there are a great many differences between school projects and "real world" projects. In the "real world," software engineers and programmers other than the originators must be able to understand, revise and maintain programs readily and without resorting to "re-engineering" strategies. I wonder how Mr. Ts'o's group would have fared if in the middle of the course, the instructor had introduced major changes to the program requirements AND REQUIRED PAIRS OF WORKING GROUPS TO EXCHANGE PROJECT MATERIALS OR SCRAMBLED THE GROUPS. Or what if the instructor had given them a set of unclear requirements and graded the groups on how well they elicited and met a set of "hidden" requirements. Like it or not, that is the way the software business really works.

My point? Software engineering is more than producing functional programs and "error free" code although these abilities should be prized. Error free code is meaningless if it implements the wrong function on useless data.

I think some of Mr. Ts'o's criticism may be justified. Version control is indeed very important, but I would have criticized the course (as described) on other grounds, which I prefer not to discuss.

As I have written before in this forum, I have a problem with certifying individuals. My concern is that certified people will be powerless without an additional economic or regulatory lever. I briefly described such a lever in risks a year or so ago. To summarize, I proposed not only individual certification but also accreditation for firms and organizations that produce "safety critical" software. A firm could not be accredited for "safety critical" systems unless it employed certified individuals and passed rigorous and comprehensive periodic reviews.

Mr. Ts'o brings up another point. He writes:

>If required to, I can parrot back all of the ``right" answers>on a written exam. Those answers would also mean very little>about how I really go about my programming work."

Effective certification would require individuals to do more than just pass a written test. As I envision it, certification would involve an apprenticeship, like the professional EIT grade or the residency for a medical specialty. True, the applicant would take a test; but he or she would also need certified professionals to attest to his or her competence (and character?). In addition, effective certification needs rigorous renewal criteria. Where public and individual safety must be ensured, I think such safeguards are reasonable. I would not, however, suggest that such standards apply to the writers of video games, word processors, general purpose spread sheets, and the like.

Mr. Ts'o goes on about guilds and unions and fostering mediocrity. Well, no system that human beings administer will be perfect. Mediocre engineers and doctors get licenses. A rational system of certification will accept the mediocre along with the excellent. The idea is to assure some minimum level of competence. Occasionally some incompetents will be certified, but certificates can be rescinded. Engineers and doctors can lose their licenses for a variety of reasons including incompetence. I do not know of any system of licensure or certification that tries to exclude top-notch people; however, most licenses are easier to obtain if one posesses certain credentials, such as an appropriate college degree and some relevant experience. I would not expect software engineering to be any different.

Frank Houston, FDA/CDRH

(These are my personal views, the customary corporate disclaimers apply.)

Software Engineer Certification (<u>Risks 10.41</u>)

Tompsett BC <bct@cs.hull.ac.uk> Fri, 21 Sep 90 12:37:05 BST

As I pointed out in Risks a while ago, the UK does have a means of certifying Software Engineers. The British Computer Society, as the Professional Society

in the UK can accredit Engineers to the qualification of Chartered Engineer (C.Eng). This is the same C.Eng qualification that is awarded to Structural Engineers, Aeronautical Engineers, Nuclear Engineers et. al. It is considered the highest professional qualification an Engineer can have. There are at present several thousand such Chartered Engineers registered through the British Computer Society and is a large proportion of their 30,000 plus membership.

Brian Tompsett MBCS, C.Eng, Department of Computer Science, Hull University

Applicability of software curricula

Jeffrey Mogul <mogul@decwrl.dec.com> 20 Sep 1990 1841-PDT (Thursday)

To back up what zzz@NISC.SRI.COM (Michael J. Konopik) writes in <u>RISKS 10.41</u>: It would seem that Theodore was so intent on blocking out the Liskov philosophy of programming that he didn't hear the statement of the purpose of 6.170. In fact, the same teaching strategy was applied in 6.001 and 6.004, as well. None of those classes taught their material using any "real world" languages or tools.

I took 6.170 (under a different number) the first time Prof. Liskov taught it, in 1978. At that time, the CLU compiler wasn't even available, so we had to code in PL/1 (which reminds me of a RISKS-type story, but that is for another day). So, not only were we being encouraged to use what some people consider an unrealistic language, but we then were able only to "pretend" that we were using CLU.

In retrospect, this was an excellent experience for me. Since then, I've programmed almost exclusively in unsafe languages (assembler, C, Pascal, Modula-2) but since I learned how to apply CLU-like discpline without being able to rely on a compiler enforcing the rules, I think my code is much better for it. (I'll also note that many of the good skills I learned in that class pertain to higher-level issues that could not be enforced by any compiler.)

This has nothing to do with whether software professionals should be certified; but I believe my experience showed me that good skills can be taught, even though some of my classmates never got the message.

-Jeff

✓ Occupational Licensing (Book Review)

Tony Harminc <ONY@vm1.mcgill.ca> Thu, 20 Sep 90 20:59:06 EDT

The Rule of Experts - Occupational Licensing in America. By S. David Young. Cato Institute, 1987. ISBN 0-932790-62-3 (paper). 99 pages.

"Occupational regulation has served to limit consumer choice, raise consumer costs, increase practitioner income, limit practitioner

mobility, deprive the poor of adequate service, and restrict job opportunities for minorities -- all without a demonstrated improvement in quality or safety."

This is the author's thesis, and he backs it up quite well in this very readable little book. Young concentrates on what might be called consumer occupations - lawyers, doctors and dentists being the most prominent. Did you know though, that 490 occupations are licensed in the United States while 643 require registration ? These range from falconers and ferret breeders to barbers and beauticians.

Conspicuously missing from discussion is engineering, which is most often held out as an example of the 'professionalism' that programmers should aim for. However the chapters 'Licensing and quality', 'Licensing and information control', 'Professionals and the scope of practice', and 'Licensing and innovation' are highly relevant even to such a supposedly non consumer-oriented business as programming.

>From the chapter 'The Demand for Licensing':

"In the public-interest theory of licensing, regulation is introduced for the benefit of the public at the urging of consumers or their agents. Government is viewed as a benevolent, if sometimes misguided, body that seeks to maximize social welfare. Regulations are imposed at the urging of consumer interest groups because regulators believe, rightly or wrongly, that efficiency or fairness or both will therefore be enhanced."

"Critics of this hypothesis believe to the contrary, however, that regulators' and professional groups' self-interest has been and still is the primary motivator of regulatory legislation. And indeed the evidence shows that consumers rarely engage in campaigns to license occupations. If the purpose of licensing were to improve the quality of service, one would expect consumers, who might be the prime beneficiaries, to promote licensure, but licensing is systematically promoted by practitioners ..."

The book has over eighty references -- most from the US, but several from Canada and Europe. A number of these attempt to make the case *for* licensing, which Young generally demolishes quite effectively.

Recommended reading.

Tony Harminc, Ultramar Canada Inc.



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 10: Issue 43



Arbitration Myths (Peter Denning, <u>RISKS-10.42</u>)

Leslie Lamport <lamport@src.dec.com> Mon, 24 Sep 90 10:36:11 -0700

Peter Denning correctly observes:

The fundamental theorem of arbiters is: There is no fixed time bound for the arbiter to make its choice.

It may make things a bit clearer to phrase this as follows. A designer of a circuit that has an arbiter has two choices:

1. Have his circuit wait arbitrarily long for the arbiter to make up its mind, thereby guaranteeing that his digital circuit elements will operate digitally, "seeing" only 0's and 1's.

 Bound the length of time the circuit waits for the arbiter, thereby introducing the possibility that his digital circuit will behave like an analog circuit, with 1/2's flowing along the wires, and do strange things.

Peter then asserts:

Lamport showed how to achieve fair mutual exclusion without any requirement that references to memory cells are arbitrated (1974).

While perhaps correct, this statement is misleading. The bakery algorithm achieves mutual exclusion without assuming any arbitrated access to memory. However, reading a memory cell that may be written while it is being read requires that the reader have an arbiter. (The reader needs an arbiter to decide whether the change from 0 to 1 occurred before or after a read operation.) In fact, the mutual exclusion problem is characterized by the fact that any solution requires an arbiter. (It is a testimony to Dijkstra's insight that certain requirements set down in his original 1965 paper, apparently regarded as irrelevant and omitted by others in later statements of the problem, are necessary to distinguish mutual exclusion from theoretically easier problems that can be solved without an arbiter.)

As Peter observes, the only way to build a computer that is safe from "arbitration failure" is by making choice 1, which means that the computer must turn off its clock while waiting for an arbiter to decide. Note that the computer can't keep its clock ticking while waiting for the arbiter to make up its mind, since it would then require another arbiter to decide within the current clock cycle whether or not the first arbiter had made up its mind. I know of no computer that turns off its clock in this way. Moreover, doing so necessarily eliminates the possibility of fault-tolerance. Omission faults can be detected only by time-out, which means by keeping a clock running. Thus, a system that is impervious to arbitration failure cannot be fault-tolerant.

Thus, Peter's

Conclusion: we know how to build fair arbiters and how to design circuits that are free of synchronization errors.

is again perhaps correct, but misleading. We know how to design those circuits, but we also know that they are impractical.

Having said all this, I should now add that the situation, although hopeless, is not serious. We cannot make circuits with no theoretical possibility of arbitration failure, but we can make them with no practical possibility of such failure. By arguments that would constitute a proof to a physicist, and a joke to a mathematician, I think one can show that if a circuit has normal reaction time of order T0, then an optimimum arbiter has probability about e^(-T/T0) of not having reached a decision by time T. It appears possible to build such an optimal arbiter. Thus, by simply allowing enough time for the arbiter to decide, the probability of an arbitration failure can be made negligibly small.

Of course, note the "can be". How many of the engineers designing digitial

circuitry are aware of the problem? Once, in the late 70's or early 80's, I had the horrifying experience of spending 1/2 hour trying to explain the problem to computer designers at Bendix, with an utter lack of success.

Leslie Lamport

P.S. People interested in the arbiter problem might like to read my unpublished paper "Buridan's Principle", available by request.

Arbiters and glitches

"Mark S. Day" <mday@brokaw.LCS.MIT.EDU> Sat, 22 Sep 90 18:34:11 EDT

Peter Denning is absolutely right (in <u>Risks 10.42</u>) to correct the claim that "it is impossible to build a fair arbiter." However, the fact that reliable arbiters are possible is quite different from saying that they are implemented in most systems.

As Denning's "fundamental theorem of arbiters" shows, the interface between an asynchronous system and a clocked system is a source of unreliability (not unfairness) and it is not possible to eliminate glitches except by eliminating the interface (using an entirely asynchronous system). The probability of glitches can be reduced, but only by reducing the performance of the interface (lengthening the decision time). The original writer might well have been assuming clocked systems (which are, after all, the vast majority of digital systems in the world) in which case there is an important kernel of truth to the original claim of impossibility, even though it is indeed technically incorrect.

--Mark Day

✓ Overbilled by 6 orders of magnitude

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Sat, 22 Sep 90 16:32:21 PDT

Excerpted from the 9/21/90 San Jose Mercury-News:

PHONE BILL'S WRONG NUMBER: \$8.7 MILLION

Chicago (AP) -- Cori Ward's mother got a little defensive when she received a phone bill for three weeks' service -- \$8.7 million.

"She says, 'I only called my sister," said Ward, who handles her elderly mother's bills.

The bill from Illinois Bell should have read \$87.98, not \$8,709,800.33.

•••

Ward said she had a hard time explaining the mistake to the phone company.

The error occurred when someone incorrectly typed a "correction" into the computer system, said Larry Cose, a Bell spokesman.

Kisks of "automated guided vehicles"

<pine_ridge%oak.span@Sds.Sdsc.Edu>
Mon, 24 Sep 90 12:07:24 GMT

Excerpted from the Maryville/Alcoa (Tenn.) _Daily Times_, September 10, 1990, p.1. :

ALCOA Worker Killed

Donnie W. Britton, 48, of Madisonville, a 24-year employee of ALCOA, died shortly before noon Saturday at UT Hospital following an accident at ALCOA's North Plant.

Elton Jones, ALCOA's director of public relations, said Britton, an electrician, was working on an overhead crane that was not operating when the crane's tray grab, the part that hangs down and lifts trays of coils (of aluminum sheet), was struck by the top of a coil being transported at ground level by an automated guided vehicle. The impact caused the crane to move toward Britton who was crushed between an access platform on the crane and the personnel lift he had used to reach the crane

This looks to me like (1) poor work practice and (2) poor a.g.v. design. Comments?

Brad Dolan, Science Applications International Corp (my opinions) pine_ridge%oak.span@sds.sdsc.edu bdolan@cup.portal.com

Field commanders using UNIX?

<twb@hoqaa.att.com> Mon, 24 Sep 90 16:28 EDT

I came across this in a news digest. As you can see it is attributed to UNIX Today:

> "To combat the use of chemical weapons by the Iraqis, the Pentagon is planning a two-pronged, high-tech defense using UNIXbased laptops. Using meteorological-type programs, the laptops could quickly determine how widespread the attack will be, where the troops can safely be deployed and how quickly they should be moved. The information would then be fed into UNIX-based PCs, and field commanders would run a variety of attack scenarios. A full meteorological model, able to forecast likely future wind
conditions over the entire risk area, could be generated within 60 seconds. [UNIX Today, 9/17/90]"

Field commanders using UNIX? Meteorological models in 60 seconds on a Unix-based laptop?

Tom Beattie att!hoqaa!twb t.w.beattie@att.com

[Whether it's cold, or whether it's hot, weather is weather, whether or not. It's known as whethering the storm. PGN]

Re: Expert system in the loop (Thomas, <u>RISKS-10.37</u>)

<jaffe@safety.ICS.UCI.EDU> 24 Sep 90 19:06:26 GMT

>Martyn Thomas reports:

<>According to Electronics Weekly (Sept 12th, p2): [...]
>In fact, he has contradicted his own assertion that the AEgis system was
>responsible by pointing out the shortcomings in human judgement, human
>psochology, and human I/O. The principal (and significant) shortcoming
>of AEgis in this scenario is that its database apparently did not
>include a readily available schedule of commercial airline flights for
>the region in which AEgis was deployed.

I was one of the principal designers of the MMI for Aegis so I have read the past and current discussions on this subject with some interest. A couple of years ago PGN posted a summary of some remarks I made on the subject of the Aegis MMI at an informal sidebar to one of the sessions of the 5th International Workshop on S/W Specification; I won't repeat them here - interested readers are referred to the Risks archives.

[See <u>RISKS-8.74</u>, 26 May 1989. It was a really fine item, and it also appeared in ACM SIGSOFT Software Engineering Notes, vol 14, no 5, July 1989, pp. 20-22. PGN]

Here, I only want to interject a comment on the more recent post extracted above. It is certainly true that Aegis as originally deployed did not include a database of commercial flight data. I recall some informal discussions about that possibility at the time. Our Navy customer had not specified anything like that in their requirements, but the possibility was mentioned by me (and others), none-the-less. There were several reasons why it was not further pursued:

(1) Philosophic disagreements on the nature of probable Aegis employments. In a blue-water, all out conflict, commercial flight data processing would be irrelevant and unused. The Navy did not want to spend scarce development funding on what they perceived of as marginal requirements. It is my personal perception (shared, I'm sure, by many others) that the armed services tend to design systems for "pure" threats and scenarios. Aegis was conceived of as providing defense for the carrier task force in open water conflicts. The then recent experiences of employing missile cruisers in close in the Gulf of Tonkin (NORSAR and PIRAZ, specifically) seemed to be regarded as an aberration: "Vietnam was a mistake; we won't make that mistake again; no more confused little conflicts for the U.S." We often heard the sentiment that we (Navy and contractor jointly) did not want to be guilty of the oft repeated mistake of designing systems to meet the requirements of the last war. The risk, of course, was and is that we could fail to institutionalize what some of us so painfully learned from our experiences.

(2) Logistic/design problems relating to the complexity of flight data processing (keeping track of commercial flight plans and correlating real-time tracks with possible flight plans). The Navy did not then (nor I presume does it now) have any facilities aboard tactical vessels for obtaining and distributing commercial flight plan data. The resources required are significant, both personnel and computational. At the time, the Navy was under intense pressure to reduce manning requirements for the Aegis ship. I also doubt whether the UYK-7 technology of the day could have handled the computational load required. There also would have had to be additional communciations bandwidth dedicated to the distribution, update, and coordination of flight data. In those days, digital bandwidth to ships was extremely limited (it almost certainly still is).

The point is that the issue of designing Aegis to handle commercial flight data was addressed and rejected as not cost-effective. Whether one agrees with this specific decision or not, the general point is that no military system (or any system) can be designed to deal with all contigencies that someone thinks of as appropriate. All the ideas that the anyone on the team came up with got discussed, some were selected, some were not. As always, the operational users wound up having to make do with a system that was not optimized for the environment in which they found themselves and whose limitations neither they nor the policy decision makers who directed them fully understood. I am still not sure whether any of the "what-ifs" represent design flaws or shortcomings.

Expert system in the loop (Henry Spencer, <u>RISKS-10.42</u>)

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Mon, 24 Sep 90 11:36:46 PDT

> the Pentagon's finding was not that nobody

> was responsible for the [Vincennes] mistake, but that no *blame*

> was attached to the captain and crew as a result of it...

> The [military's] job is to carry out the policies of

> their government, and if innocent people get hurt, that is

> the policy- makers' problem....

Since the Vincennes' very mission was to keep the Gulf safe for civilian traffic, the point argued by Henry here, even were it elsewhere valid, in fact weighs against his argument that Captain Rogers' reasonably decided to risk civilian life. As for the the general case, there certainly are regulations drawn up in international law, that protect civilians from risk, even in battle. (An air embargo against Iraq cannot now be *enforced* under this sort of international law.) Likewise, a suit filed in international court in Costa Rica against the U.S., for its bombing of a civilian mental hospital in Grenada, was *settled* by the U.S. (albeit without admission of blame). In brief, the U.S. would have had to show sufficient probable cause for the bombing, by objective standards, had trial been reached.

<>>In the case of the Vincennes, it cannot be disputed that a mistake <>>was made. The Pentagon found no human responsible for it, so it <>>must have been a mechanical error.

> This statement is in error. Please, READ THE REPORT . . .

> The board found that Captain Rogers made a correct decision to fire> based on the data that he had available to him.

The data was generated by computer, and the misinterpretation of screens that occurred was deemed foreseeable (and was forgiven) in the circumstances. I fail to see even a small error in my claim, let alone a capitalized error. Given the facts, which we agree on, it is a matter of definition as to whether we say that the computers "made" the decision to shoot, which is the definition I assert as a matter of commonsense and law.

<>>Such decisionmaking is de facto *governed* by computer: without <>>computer prompts, no retaliatory decision at all would be taken; > Again, incorrect. Decisions to fire were made long before we > had computers -- they are not required to make these decisions.

Well, yes, but I'm not saying that mistaken visual identification is a computer error, I'm talking about decisionmaking taken by commanders whose only inputs are computer screens of information. There's a qualitative difference, though I agree that drawing the line meaningfully is not easy, it's clear to me that momentary decisions taken in the Vincennes windowless control room are properly deemed computer-governed.

vincennes incident (Henry Spencer, <u>RISKS-10.42</u>)

Wheels in Wheels <bahn_pr%ncsd.dnet@gte.com> Mon, 24 Sep 90 16:28:18 -0400

I believe Henry failed to observe a key point in the navy review of the Vincennes incident. The Assistant Anti-Air warfare officer failed to set the range gate for the IFF unit to allow for the changing distance to the target. Consequently instead of pinging the transponder on the A300, they were pinging an F-14 on the ground at Bandar Abbas. Also no consideration was given that F-14 lack an anti-ship capability.

The Radar operator also mis-read his screen, interpreting range for altitude, and also was unaware of the fact that a civil air corridor ran through the gulf, and that the A300 was in fact in the center of the corridor. The Vincennes lacked VHF radios to interrogate Iranian Civil air also. Civilian aircraft at 33,000 feet are also by definition well clear of ships, and probably would not even be able to identify them without optical instruments.

As I read the Navy report, there were two distinct personnel failures by Vincennes crew, compounded by Inability to interrogate the A300. The Navy review board faulted the design of the screens for not presenting information in a clear manner. Heat of battle was also considered a mitigating factor.

What is not understood by readers of Risks, is the Persian gulf is an exteremely busy commercial zone. Hundreds of Planes and Boats ply those waters every day. To shoot at every moving target is negligent on our part. THese systems are designed for high intensity combat with dozens of combatants and numerous inbound threats. Trying to pick out a single hostile among hundreds of non-combatants is a much more difficult task.

The Iran-Iraq war contrary to one readers opinion was not WW2. In WW2, there were clear sides. CLearly marked hostile zones and very few nuetrals. WW2 was also a total war. No tactic was untried save for Gas. THe Iran Iraq war was a relatively small war between tow neighbors in a very crowded environment. Interjecting High strung war ships into such an environment was only bound to cause such errors.

THe Stark had made a type 2 error. Actually hostile, Failed to shoot. THe Vincennes made a type 3 error. Actually Civil, Did shoot.

I am sure in the mind of the captain of the Vincennes was the court martial of the Stark's captain and his claim that the electronic systems had failed to identify the threat, increasing the probablity now of a type 3 error.

While the Navy review board did reccomend changes involving Man-machine interfaces, knowledge of commercial routes, Addition of VHF radios and upgrading of the IFF system. I feel the fundamental error was placing military vessels into a environment crowded with non-combatants. These vessels are designed to fight WW3, not police brush-fire wars. This was a major problem for US troops in Vietnam also.

Apollo, The Race to the Moon

<cook@csel1.eng.ohio-state.edu> Mon, 24 Sep 90 15:06:54 EST

The excellent book recommended by M.Minow is available in paperback for \$12.95. The reference is

Murray, Charles & Cox, Catherine B. Apollo, The Race to the Moon. Simon & Schuster, 1989. ISBN 0-671-90625-X

R.I.Cook cook@csel.eng.ohio-state.edu

Failed mail (msg.aa00705)

"helios.northeastern.edu mmdf IIb upd 43" <mmdf@helios.northeastern.edu> Mon, 24 Sep 90 0:18:31 EDT

After 246 days (5891 hours), your message could not be fully delivered.

It failed to be received by the following address(es):

nu-risks@nuhub.acs.northeastern.edu (host: nuhub.acs.northeastern.edu)...

Problems usually are due to service interruptions at the receiving machine. Less often, they are caused by the communication system.

Your message follows:

Received: from HERCULES.CSL.SRI.COM by helios.northeastern.edu id aa00705; 21 Jan 90 11:11 EST Received: by hercules.csl.sri.com at Sat, 22 Sep 90 13:26:33 -0700. (5.64+/XIDA-1.2.8.35) id AA28066 for oneil%NASA-JSC.CSNET@RELAY.CS.NET From: RISKS Forum <risks@csl.sri.com> Date: Sat, 22 Sep 1990 13:26:31 PDT Subject: <u>RISKS DIGEST 10.42</u>

RISKS-LIST: RISKS-FORUM Digest Saturday 22 September 1990 Volume 10 : Issue 42 RISKS-LIST: RISKS-FORUM Digest Wednesday 22 September 1990 Volume 10 : Issue 42

[Northeastern has always been an interesting host.]

[By the way, I am sorry about the 81-character line ending with Volume 10 : Issue 42 where many of you could not read the "2" at the end. Yes, I know, Issue 43, also. Mark Brader <msb@sq.com> pointed this out to me, and I replied with a comment such as how on double-digit Wednesdays and occasionally Saturdays in September my masthead lead could run over 80 characters (in Volume 10 and from now on, unless I am on my toes, as I was in <u>RISKS-10.36</u>.) (I've shortened the line by one character in this issue, so now it is just Wednesdays in September 1991, etc., that I'll have to watch out for. I'll set my calendar program to remind me, if I am still running RISKS then.) PGN]

"... when the moon is in the third quarter? :-)" says Mark.

"[Jupiter's] satellites are invisible to the naked eye and therefore can have no influence on the Earth and therefore would be useless and therefore do not exist." -- Francesco Sizi, quoted by T. Cox



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 10: Issue 44



<smb@ulysses.att.com> Tue, 25 Sep 90 08:20:58 EDT

A political scandal, known variously as ``Trentongate'' or ``Computergate'', is brewing here in New Jersey. A staff member employed by the Republicans in the state legislature has admitted to breaking into a computer system used by the Democrats; reportedly, the number of documents obtained is in the thousands. His activities were known to the staff director; he recently admitted as much and resigned. But the Democrats aren't making too much of a fuss over this -allegedly, they don't want the contents of the filched documents disclosed, since they are reported to deal with improper use of state facilities for political purposes. (Were Nixon's tapes 9-track, and was the 18 minute gap really part of the tape drive error recovery processing...? And Haig's ``sinister force'' was just an ordinary reboot.)

--Steve Bellovin

[Donkey haute and pancho sans a ba(s)bar tilting at winned spills? (Please pardon my espanofranglais, Sir Vantes!) PGN]

Whitehall rebuked for 121 million pound Retail Price Index blunder

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 25 Sep 1990 11:50:53 PDT

1

A 1% error in the British RPI cost the government 121M pounds in compensition to pension and benefit losers, donations to charities, and administrative costs. The problem was discovered after a computer error caused the RPI to be understated from February 1986 to October 1987. The programs had been tested, but the tests did not reveal the error.

Source: Computing (UK), 20 September 1990, submitted via airmail by Dorothy R. Graham, Grove Consultants, 40 Ryles Park Rd., Macclesfield, Cheshire SK11 8AH.

Hi-tech advertising

Dave Turner <dmt@ptsfa.pacbell.com> Mon, 24 Sep 90 22:16:39 PDT

The San Francisco Chronicle had a front page article today (09/20) headlined:

High-Tech Advertising Better Junk in New Junk Mail

A few quotes:

Junk mail is going high tech. Across the nation, well-heeled consumers are being bombarded with expensive computer diskettes, elaborate video-tapes of car commercials and even catalogs that play Christmas carols. ...

+ Compaq Computers mailed 40,000 floppy disks to possible customers last summer to introduce a new line of computers that cost as much as \$20,000. ...

Kevin Bohren, a spokesman for Compaq Computers in Houston, said his company tripled its response rate last year when it mailed "interactive diskettes" as a promotion for its new line of personal computers. "People responded because we weren't just sending out another pamphlet," he said.

If people become accustomed to inserting every floppy received in the mail into

their computers thinking that it is just another form of advertising, the risk of viruses spreading will increase rapidly. A few thousand deviant floppies sent to several large corporations and schools will produce marvelous results.

Students taking exams by remote hookups

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 25 Sep 1990 11:44:07 PDT

An AP item today was called to my attention, datelined CHICAGO (AP).

"Thank you for calling Telequiz. After the tone, please leave the answers to your college exam."

In what is believed to be the national debut of student testing via push-button phone, students at Governors State University telephoned in the answers to their Psychology 519 quiz from the comfort of home.

[True-false answers are recorded with computerized voice-mail equipment. A professor was quoted as how this saves everyone time, effort, and travel, and provides considerable convenience because students can be tested when they wish -- although in its present implementation only one student can call in at a time. No reentrant exam programs (as opposed to reentrance exams) yet! RISKS readers do not need to be reminded of the security/integrity problems. PGN]

🗡 Sun C2 system

Stephanie Zakrzewski &akrzewski@DOCKMASTER.NCSC.MIL> Tue, 25 Sep 90 09:59 EDT

I'm amazed by recent references to Sun's "C2" system. What system is this? There has been no Sun product evaluated by the National Computer Security Center, so there is no such thing as a "Sun C2 system". Like the Good Housekeeping Seal of Approval can be awarded by only Good Housekeeping, a rating against the Trusted Computer System Evaluation Criteria (the Orange Book, which defines C2 and the other levels of trust) can be awarded only by the National Computer Security Center, which authored the Orange Book.

Each product which has been evaluated and thus earned a rating is announced in the Information Systems Security Products and Services Catalog, chapter four, the Evaluated Products List. So if you are in doubt in future, check this source. Anything not in there is, at best, DESIGNED TO MEET C2. At worst, it provides no trust at all. Don't be misled by premature or misleading claims. Relying on false security is far more dangerous than having no security - at least in the latter case you stay on guard!

🗡 Arbiters

Brian Randell &rian.Randell@newcastle.ac.uk> Tue, 25 Sep 90 10:47:26 BST Nearly twenty years ago David Wheeler of Cambridge University, lectured here on this subject in our Annual International Seminar on the Teaching of Computing Science at University Level (7-10 Sept. 1971). RISKS readers might enjoy this quote from the Seminar Report:

"The Problem of Synchronisation

Dr Wheeler devoted the rest of his talk to a discussion of a particular problem in logical design. He chose to do this, rather than give a more general talk, because he considers that discussion of this point should form part of every course on hardware or logical design. His reasons for emphasising this point, which he calls the problem of synchronisation, are as follows:

- (a) Many existing computers have faults because of neglect of this point. (Dr Wheeler found that at least 50% of the computers whose logical design he has studied in detail have faults of this kind.)
- (b) The point is rarely taught well and only occasionally appears in text books.
- (c) It is apparently difficult to to appreciate. Furthermore, people trained in switching theory or logical design find it especially difficult.
- (d) The problem is general. It is common to all forms of logic and may also be present in systems programs. It touches many disciplines, for example circuit theory, logical design, systems programming and information theory.
- (e) The occasional malfunctioning of all practical computers and peripherals is to be expected if this point is neglected."

[The report then goes on to give a detailed account of David Wheeler's lecture.]

(Younger RISKS readers may not be aware that David Wheeler, who I'm pleased to say is still very active, was in 1949/50 the principal source of such concepts as closed subroutines, assemblers, post mortems, and much else, in his pioneering programming work on EDSAC, and went on to do much hardware design, for example of EDSAC2 and of the Cambridge Ring.)

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK PHONE = +44 91 222 7923 FAX = +44 91 222 8232 Brian.Randell@newcastle.ac.uk

Re: Expert system in the loop (Thomas, <u>RISKS-10.37</u>)

Amos Shapir <amos@taux01.nsc.com> 25 Sep 90 15:50:52 GMT

[Quoted from the referenced article by jaffe@safety.ICS.UCI.EDU] >The point is that the issue of designing Aegis to handle commercial flight data

>was addressed and rejected as not cost-effective. Whether one agrees with this >specific decision or not, the general point is that no military system (or any >system) can be designed to deal with all contigencies that someone thinks of as >appropriate.

The point is, I don't think Aegis had to be designed to keep track of all aerial traffic in the area; I'm pretty sure that *Air Force* systems in the area did have a positive ID on everything that was flying at the time. The trouble is, I also suspect that there was no way the captain could just call somebody and ask "Hey, what's that on my screen?"

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522255 TWX: 33691, fax: +972-52-558322 amos@nsc.nsc.com

Expert system in the loop (Aegis display)

Jim Horning <horning@src.dec.com> 25 Sep 1990 1252-PDT (Tuesday)

The renewed discussion of the Vincennes incident brought back some 25-yearold memories about displaying aircraft tracking data. I don't think this problem has been discussed in RISKS (at least not recently):

The risk of displaying data that was computed for a different purpose.

I have no reason to believe that there's any direct connection between the following story and the Aegis system--I'm only saying that the Aegis developers must have faced the same kind of problems.

At that time, I was supporting myself in graduate school by programming for a major aerospace manufacturer. I worked on a weapons guidance system that I've heard is still used in top-of-the-line US combat aircraft. I was responsible for displaying the tracking data. Newsweek published a picture of an Aegis display that included the same track symbols as we were using, but that probably just means they are some kind of a military standard.

Before testing our software with real sensor data, we ran numerous tests with simulated data. It quickly became apparent that the velocity displays were unacceptably erratic, and didn't have much connection to the velocities of the simulated targets. So we simplified the data to a single target moving in a straight line with no acceleration. Still looked awful. So we reduced the simulated sensor noise, and finally eliminated it. The velocity display was a lot smoother, but it showed target velocities and maneuvers that just weren't in the input.

Finally I decided to do a little mathematical analysis. I was able to identify two sources of error in the second-order difference equations used to smooth and extrapolate track data:

- Sensor data was supplied in polar coordinates, and all calculations were done in polar coordinates. In general, unaccelerated straight-line

motion produces non-zero derivatives of all orders in polar coordinates. At the ranges and velocities for which the system was designed, these virtual velocities and accelerations were not negligible.

- The smoothing algorithm initialized the first and second difference estimates on all coordinates of a track to 0. At the ranges and velocities for which the system was designed, the differences could start from zero, overshoot, overshoot in the other direction, ... and not stabilize within the time a straight-line target remained in range.

I was able to show that a straight-line target 60 miles away that was moving perpendicular to the tracking plane could have an indicated velocity 90 degrees off its true velocity, i.e., the display would show its velocity as being straight towards the tracking plane. I didn't think that such a velocity display was likely to help the Missile Control Officer make good decisions.

Our department was only responsible for the software. I wrote up my analysis, including a demonstration of the improvements that would result from smoothing and extrapolating in a cartesian coordinate system and from initializing the differences more reasonably. I sent my analysis off to the department that had supplied the smoothing algorithm, feeling very proud of my young self for having caught the problem and figured out the solution before it caused any real trouble. But the answer from that department was: "We don't understand your mathematics. We optimized the algorithm using Z-transforms, and it's not your job to second-guess us." (This was one of several reasons why my career in aerospace was brief.)

Later, I learned that the algorithm was not as unreasonable as it had seemed to me. The primary purpose for maintaining the track files was to lock a missile's sensors onto a particular target before launch, and the sensors had to be aimed in polar coordinates.

The real problem was that someone designing the man-machine interface had seen that the track file format contained fields R, RDOT, RDDOT, etc., and decided that, since the velocity information was available, it would be a good idea to display it for the MCO. But it wasn't a good estimator of velocity, and was never designed to be.

To me it is entirely plausible that the junior officer on the Vincennes who made errors in reading the altitude and speed of the approaching aircraft was in fact being misled by the displayed velocity, and not just by stress. I doubt that the logging data for the Aegis records enough of what is displayed at each instant to settle this. Doubtless some readers of RISKS know enough about the Aegis software to know whether this is possible, but they may not be free to comment on the subject.

Jim H.

Re: Expert systems in combat

<ORN%HYDRA@sdi.polaroid.com> Wed, 26 Sep 90 10:57 EST Various people have commented on Vincennes incident without noting the applicable international law. This law, which has counterparts running back over a century, places the responsibility for identification upon the *CIVILIAN*. The military is permitted to presume hostile intent from all unidentified people or things in a combat area. The civilians must demonstrate by words and actions that they are non-combatant. Transponder codes are explicitly listed as not sufficient.

In the particular case of the Vincennes, the military did comply with the law by issuing a challenge and demand for course change. Unfortunately the aircraft ignored this challenge (probably because it was to ``unidentified aircraft'' and in nautical phraseology). And for these reasons there has been no real effort to condemn the action in any court of international law.

This is not to say that problems and errors did not occur. One problem that an expert system might have resolved would be a more universal and internationally understandable challenge terminology. It took the shooting down of two airliners by the Soviets to force general installation of mutually usable radios in both military and civilian aircraft. This accident reveals that despite mutually usable radios, there remain significant communications difficulties. (Not the original mentioned use for expert systems, but much easier and well within the present state of the art.)

The other risk that this shows is the danger of fundamental ignorance of overall environment. International law and treaties do exist, and do matter, but both within this group and within the developers of the expert systems there is profound ignorance of these rules. When the rules are in software or hardware what do you do when treaties change?

R Horn horn%hydra@polaroid.com

Reliability of the Space Shuttle

Peter da Silva <dasilva@ficc.ferranti.com> 25 Sep 90 15:29:32 CDT (Tue)

Not attempting to address other issues involved in the article by Perry Morrison in comp.<u>risks 10.40</u>, I would like to simply point out that the space shuttle has had many more successful launches than any other launch system employed to date. The shuttle, as a whole, is extremely reliable... it can only be considered a failure in comparison with the outrageous levels of reliability *claimed* for it by NASA prior to the Challenger accident.

🗡 Illinois Bill

Mark Brader <msb@sq.com> Tue, 25 Sep 1990 22:31:19 -0400

> The bill from Illinois Bell should have read \$87.98, not \$8,709,800.33.

Hmph. That's only 5 orders of magnitude.
Mark Brader, Toronto utzoo!sq!msb, msb@sq.com
[So what's an order of magnitude here or there? Thank goodness it wasn't an earthquate. PGN]
Image: Image: PGN Image: P



Nathaniel Borenstein <nsb@thumper.bellcore.com> Fri, 28 Sep 1990 11:22:52 -0400 (EDT)

Because of a software screwup, the lottery database system let 6 winning tickets be purchased after the winning numbers had been drawn in the Tri-State Megabucks game for Vermont, New Hampshire and Maine. There was one legitimate ticket for \$1.1 million. The problem was caught before any payoffs could be collected. In addition, some belated daily lottery ticket winners did collect, up to \$5,000, although the state is apparently insured against the loss. The system is supposed to halt ticket sales 10 minutes before the drawings, but did not. [Source: an AP item by Frank Baker, 28 Sept 90, summarized by PGN]

✓ Safer to Fly or Drive?

David Levine <levine@crimee.ICS.UCI.EDU> Thu, 27 Sep 90 11:02:13 -0700

The following is extracted [and with edits by dll] from Daniel J. Holt's editorial in September 1990 _Aerospace Engineering_. Holt summarizes the paper "Is it Safer to Fly or Drive" by Leonard Evans, Michael C. Frick, and Richard C. Schwing of General Motors Research Labs, published in _Risk Analysis_, Vol. 10, No. 2, 1990. The statistics, and more specifically some of the assumptions behind them, may be of interest.

[...] Apparently the researchers found fault with the cliche that the most dangerous part of an airline journey is the drive to the airport. Over 98% of the intercity travel in the U.S. is via airline and automobile. On a daily basis, 18,000 airliner takeoffs and landings and 370 million mile car trips are completed in a safe manner.

[claim commonly quoted fatality rates of] 0.6 deaths per billion miles of flying and 24 deaths per billion miles of driving. Specifically, they claim these rates are incorrect for three reasons:

- -- The airline rate is passenger fatalities per passenger mile, whereas the road rate is all fatalities (all occupants, pedestrians, etc.).
- -- Road travel that competes with air travel is on the rural interstate system, not average roads.
- -- Driver and vehicle characteristics, and driver behavior, lead to car-driver risks that vary over a wide range.

[... 40 year-old, seat-belted, alcohol-free drivers (do they assume alcohol-free *other* drivers?)] are slightly less likely to be killed in 600 miles of rural interstate driving than in regularly scheduled airline trips of the same length. For 300-mile trips, the driving risk is half that of airline trips of the same length. Thus the researchers concluded that for this set of drivers, car travel provides a lower fatality risk than air travel for trips in the distance range for which car and air travel are likely to compete.

As for the cliche that the drive to the airport is riskier than the flight, the researchers concluded that average drivers with the age distribution of airline passengers are less likely to be killed on a 50-mile, one-way trip to the airport than on the flight.

David L. Levine, Dept. of ICS, University of California, Irvine Irvine, CA 92717 BITNET: levine@ucivmsa UUCP: {sdcsvax|ucbvax}!ucivax!levine

Ke: Expert system in the loop (Henry Spencer, <u>RISKS-10.42</u>)

Matt Jaffe <jaffe@safety.ICS.UCI.EDU> 26 Sep 90 20:02:46 GMT >The data was generated by computer, [...]

>>>Such decisionmaking is de facto *governed* by computer: without>>computer prompts, no retaliatory decision at all would be taken;<> Again, incorrect. Decisions to fire were made long before we<> had computers -- they are not required to make these decisions.

The term "prompt" is one key to some understanding of this type of situation. Aegis (and similar USN combat systems) is designed to permit tactical decisions to be implemented through Aegis mechanisms via three modes:

- (1) Automatic the digital system itself makes the decision
- (2) Semi-automatic (a bad name, but retained for historic reasons) - the digital system specifically prompts the operator with a specific, recommended decision, e.g., "recommend engagement of target X with weapon Y"
- (3) Manual the system provides controls to allow an operator to implement a decision

The Vincennes incident involved a manual decision. One might reasonably ask to what extent was the "manual" decision conditioned by the data presented by Aegis. Here the observation about the "windowless control room" is valid but there are still several gradations possible. If, for example, Aegis were to have routinely displayed "automatically" computed threat rankings in a color coded format (Aegis did not do that then; I doubt that it does it now), a decision to engage based upon viewing a target in blinking bright red (with all other targets being a steady, soothing blue) would still officially be a "manual" decision but certainly much more "computer governed" than a similar decision based on viewing a screen with all targets a homogeneous blue. (It is also possible - although not a factor in the Vincennes incident - for a system to provide controls for the implementation of decisions made manually based on data not mediated at all by the action-implementing system.) The Vincennes incident involved misinterpretation of displayed data, not interpretation of misleading or provocatively displayed data. (Of course, the data could be wrong; more on that in a minute.) My personal opinion is that the Captain of the Vincennes would probably have made the same decision had the same data been printed out for him in narrative text form. (That is the apparent significance of the Navy's finding that the Captain made the "correct" decision based on the data available to him.) The real issues are three fold:

- (1) How "true" was the digital systems "view" of reality?
- (2) Given the state of the art in algorithmic reasoning, could the digital system have been designed to model (I will NOT say "understand") reality any better?
- (3) How good was the MMI at presenting the digital "truth"?

For question (1), the answers appears to be mixed. The system reported a Mode II SIF on a target that did not (ignoring paranoid possibilities) in fact have a mode II capability. The altitude readouts were apparently correct.

For question (2), it is my personal opinion that the system was designed as well as we could do so at the time. The reasons for the SIF mis-assignment I and others have already discussed in other correspondence. I do not know of any design decision we could have made differently that would have prevented this error. The altitude reports were as accurate as the underlying sensor technology permitted. (Reasons for not trusting Mode C height, if it was available, were also discussed previously and should be reasonably obvious - if one believes a target might be hostile, one cannot place too much credence in data the target itself provides.) Providing a better Z resolution would have significantly increased the direct and indirect costs of a sensor already critiqued (at that time) as far too expensive. Given the inherent limits on instantaneous height measurements and the inherent manuverability of aircraft in the Z axis, Z' (rate of ascent or descent)information will generally remain highly inacurrate.

It is question (3) then, that is the heart of the matter to me. I don't have the time here to fully recap all the issues, but I would like to summarize my conclusions to date:

(1) We gave a lot of thought and discussion to the Aegis MMI. We had good engineers, MMI experts, operationally experienced Naval personnel, lots of review and open, no-holds barred discussions. We may have been wrong (I am still unconvinced, but in the sense that I don't know, not that I am sure we were right.), but we were as methodical and as careful as we could be. (2) We might have tried to find a way to display the age of last correlated IFF hit (per mode) - that would have suggested that the target was not CURRENTLY squawking mode II (but was still squawking other modes) - but we were awfully tight on display space and the Navy and our own MMI experts were already telling us that we were displaying too much data. (3) I don't think we could have done much about the Z' problem, although I have not read the Navy's report to see their specific criticism or suggestions. (I would be grateful to anyone willing to mail me a hard copy version - or reference to a classified document identifier.)

I believe that there were two classic technical problems involved in the Vincennes incident (as well as the political decision making ones well discussed elsewhere):

 How to make available and prioritize for tactical operators the display of all the information that might be of significance some of the time without constantly saturating them all the time with displays and controls that are not currently relevant.
 How (or whether) to display probabilistic and uncertain data to humans for used in highly stressed decision environments.

There is also the issue of training and comprehension, which straddles the boundary between technical and institutional: How to ensure that key decision makers (shipboard as well as policy) understand the limits of the technology that they are employing?

It is our limited ability to answer these questions that makes incidents like the Vincennes shootdown inevitable.

Ke: Expert system in the loop (Thomas, <u>RISKS-10.37</u>)

Matt Jaffe <jaffe@safety.ICS.UCI.EDU> 26 Sep 90 20:33:49 GMT

>Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel
>[Quoted from the referenced article by jaffe@safety.ICS.UCI.EDU]
<>The point is that the issue of designing Aegis to handle commercial flight data
<>was addressed and rejected as not cost-effective. Whether one agrees with this
<>specific decision or not, the general point is that no military system (or any
<>system) can be designed to deal with all contigencies that someone thinks of as

>The point is, I don't think Aegis had to be designed to keep track of >all aerial traffic in the area; I'm pretty sure that *Air Force* systems >in the area did have a positive ID on everything that was flying at >the time. The trouble is, I also suspect that there was no way the captain >could just call somebody and ask "Hey, what's that on my screen?"

Good point, with a couple of caveats:

(1) Aegis was designed to "keep track" of everything in the area. Aegis was designed to integrate identification information from all digitally accessible systems. Your comment is equivalent to asking, "Did the Captain avail himself of other possible sources of information?"

(2) You are presumably referring to AWACS; I don't know if there was an AWCAS bird covering that area at that time.

(3) I'm not an AWACS expert; I doubt that they process commercial flight plans, though. But they might not have had the mode II SIF confusion the Vincennes did.

(4) The time pressure the Captain felt he was under would be a factor (assuming there was an AWACS bird available). One would have to consider the time to make the call (depending on the tactical comm plan in effect, that could be simple or could be tough) and the perceived likelihood that the callee could tell one something that one did not already know.

So there probably was a way to call; the questions are instead, was there anyone useful (in the Captain's mind) to call and did he feel he had time to do it? The asking "Hey, what's this on my screen?" is solved procedurally, although to be fair, the actual use of such procedures (common coordinates and pro-words) with the Air Force may or may not have been something the Vincennes felt comfortable with.

✓ bookkeeping error begs for machine help -- maybe

Jim Purtilo <purtilo@cs.UMD.EDU> Wed, 26 Sep 90 21:17:31 -0400

Not yet a computer-related risk, but food for thought from today's Post:

- > Md. Admits Freeing Inmate Later Held in Three Slayings
- > by Richard Tapscott
- > Washington Post, September 26, 1990.
- >

> Maryland corrections officials conceded today that an error led to the early
 > release of a Harford County man who is charged in three killings committed
 > during a time he should have been in prison.

> During a legislative hearing today, an attorney for the Division of
 > Correction said the state could be sued by relatives of the victims if John
 > F. Thanos's release 18 months early is found to have been caused by
 > negligence.

>

> Until today, corrections officials had said only that they were
 > investigating whether there had been proper application of a complex set of
 > guidelines used in determining how much time to deduct from Thanos's
 > sentence for good behavior. "Good Time" is awarded as a method of
 > maintaining discipline in prisons and to ease crowding.
 >

> But Bishop L. Robinson, secretary of public safety and correctional
 > services, told lawmakers this afternoon that Thanos was "erroneously
 > credited" with 543 days of good conduct.

The article continues, noting that the chap served four years of a seven year sentence for robbery. Since the release, he has been charged with two murders, an attempted murder and two robberies. The attempted murder charge could be upgraded as the victim has since died.

Robinson points out in the article that corrections officials have a "monumental problem" in calculating good time under incentive programs linked to behavior, work, education and prison crowding. "The difficulty is compounded ... when overlapping or concurrent sentences are involved."

Refreshingly, a `computer error' is not yet being pointed to as the problem. But as I read this, I have visions of politicians looking for ways to automate the process `to avoid this tragedy in the future.' Should this occur, one wonders how to design the bookkeeping problem so it fails safe. Regardless, we have yet another example for my software engineering class who occasionally will ask ``why do I care about fancy techniques to test a spreadsheet -- its not like I'm writing a program that lives will depend upon.''

When the system dumps core, just dial 911, right? Jim

Re: Hi-tech advertising

Brinton Cooper <abc@BRL.MIL> Wed, 26 Sep 90 17:04:50 EDT

Dave Turner reports on advertising in which floppy disks touting some product are "junk mailed" to our homes. He correctly observes:

"...the risk of viruses spreading will increase rapidly. A few thousand deviant floppies sent to several large corporations and schools will produce marvelous results."

I've been reading RISKS-Digest for several years and (erroneously?) consider myself well-informed on topics of interest here. Yet, as I read Dave's item, the risk which he states so well DID NOT OCCUR TO ME UNTIL I READ HIS LAST PARAGRAPH! This leads to one of two conclusions:

a. In spite of our good efforts to be vigilant, the plethora of new methods of attack overwhelms our defenses.

b. I turn off my thinking apparatus when reading e-mail.

In case it's "a," many of us need to be more wary.

_Brint

Re: Reliability of the Space Shuttle (<u>RISKS-10.45</u>)

Chris Jones <clj@ksr.com> Wed, 26 Sep 90 16:44:52 EDT

I would like to simply point out that the space
 shuttle has had many more successful launches than any other launch system
 employed to date.

Hardly. The US space shuttle has had many more successful launches than any other launch system for US manned spacecraft. Almost every Soviet launch system has had many more successful launches (including the SL-4, used to launch every Voskhod and Soyuz manned spacecraft), and many US unmanned launch systems have exceeded the shuttle's totals as well.

Chris Jones clj@ksr.com {world,uunet,harvard}!ksr!clj

Reliability of the Space Shuttle

<henry@zoo.toronto.edu> Thu, 27 Sep 90 13:03:43 EDT

>... I would like to simply point out that the space
 >shuttle has had many more successful launches than any other launch system
 >employed to date...

Surely Peter jests. The Soviet "A" booster, in several variants, has been launched successfully over 1000 times. This is more than all Western launch systems, including the shuttle, put together. By normal aviation standards, this is the *only* space launcher that has been properly tested. (A new aircraft typically flies hundreds or thousands of times before it is released to customers.)

Perhaps he meant only Western launchers? Even there, this is grossly wrong. The user's manual for Scout, the smallest of the "traditional" US boosters, lists 77 successful launches. I'm fairly sure that Delta beats that, and Atlas and Titan probably likewise.

Perhaps he meant only manned launchers? Sorry, I think the "A" booster wins again. It has launched every Soviet manned mission, from Gagarin to the Mir crews.

Henry Spencer at U of Toronto Zoology utzoo!henry

Automated vehicle guidance systems

Will Martin <wmartin@STL-06SIMA.ARMY.MIL> Mon, 10 Sep 90 13:36:06 CDT

There is a program called "European Journal" which is aired on PBS (and, I suppose, some cable channels). In the program broadcast on Sunday, Sept. 9 on KETC in St. Louis, I saw a segment on automated vehicle guidance systems that are being installed in Britain and Germany (I'd say "West Germany" but it may not be that when you read this... :-). This was a system designed to route traffic around snarls, tieups, and gridlocks, providing the driver the "best" [see below] route to a punched-in destination from the current site.

The system depends on traffic-light-mounted signal sources, which seemed to be infrared emitters. The dashboard contains an LCD-type display that has arrows displayed indicating to the driver which turn should be taken next. Interestingly, the philosophy of operations varies between the two installations. In Britain, this is a private-enterprise venture, and the spokesperson stated that their aim was to provide the driver with the best route from the driver's point of view. In Germany, this is a government activity, and the aim is to provide the most efficient traffic flow throughout the city. (I suppose individual drivers could be shunted into dead ends or off the street into a canal or something if it would make the traffic flow as a whole work better. :-) This is, of course, the RISK -- will the system's advertised philosphy be the one that really controls its operation?

The British system sounded expensive to me -- \$400 initial fee, plus a \$200 per year subscription. Interviews with potential customers didn't sound too promising; no one seemed interested in spending that much for what it would give them -- they figured they could do it well enough for themselves. Don't know what the German costs will be, or who will use it.

The point of what would happen if the driver "disobeyed" the system or violated a traffic regulation (like running a red light) was asked. The British spokesman said their system was in no way limiting; they were only trying to help the driver, and that there was no way that violations of traffic rules would be reported. No mention was made of the German situation. (I suppose the next infrared sensor/transmitter unit to pick up the offending car there melts it with a laser or something...:-)

The "fail" mode of the display, if the driver ignores the turn-indicating arrow and goes straight, for example, was interesting. It seemed to take the rejection of the recommendation as a negation of the program, and displayed a rosette of arrows pointing in every possible direction. If the thing had a voice unit, I would have expected it to say something like, "WELL! If YOU want to go your OWN way, don't pay any attention to ME! Go ANYwhere YOU like!" :-)

Regards, Will Martin wmartin@stl-06sima.army.mil OR wmartin@stl-06sima.army.mil

✓ Computer 'error' in the British RPI

&ichard_Busch.sd@xerox.com> Fri, 28 Sep 1990 10:37:47 PDT

In his Tue, 25 Sep 1990 11:50:53 PDT Peter G. Neumann quotes from Computing (UK), 20 September 1990, submitted by Dorothy R.Graham:

>A 1% error in the British RPI cost the government 121M pounds ...a computer error caused the RPI to be understated from February 1986 to October 1987. The programs had been tested, but the tests did not reveal the error.<

It is perhaps worth mentioning that the current UK Government has made control of inflation, measured by the RPI, one of the main items on its agenda, and that a General Election occurred during the stated period.

Taking this in combination with the use of the Falklands / Malvinas War for electoral purposes, with the deliberate massaging of official statistics (particularly on unemployment) since 1979, to such a degree as to cause near-mutiny in the Government Statistical Service, and with the general cynicism of the present UK Government, the uncharitable might suggest that the 'error' was no more than another episode of electoral 'management' on the UK Government's part, and that 121 million pounds would be considered a small price to pay for re-election by people as power-hungry as Margaret Thatcher.

The 'secondary RISK' of people becoming so accustomed to computer 'error' as to be willing to accept it as fact rather than to suspect deliberate manipulation of computer-resident data has already been discussed in RISKS.

Chaz



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Master Of Darkness <clee@td2cad.intel.com> Sat, 29 Sep 90 21:57:26 PDT

I just received my registration notice from the DMV (Department of Motor Vehicles). This piece of paper shows the amount of money I need to pay, so that I can drive my car for the next year in California.

Imagine my surprise when I saw the amount: \$2214. An extremely big surprise since I only paid ~\$600 last year, when I purchased the car new. The reason for this new method of making money?

This is the excuse from the clerks at the DMV. Seems that they have

just started using a new computer program for billing purposes, apparently on their new Tandem computers. Surprise Surprise it seems that everybody who got a recent registration statement, has an invalid amount. I had to go to the local office so that they could print up a new form with the correct amount. I don't know if registration statements were the only incorrect items produced. They didn't volunteer the information and I didn't ask.

Supposedly some people received bills for less then the correct amount. I wonder if they will still get their registration tags when (if) the computer notices the underpayment. Will those who might have paid too much get refunds?

BTW, the correct amount I'm supposed to pay? \$351.

Cecil Lee, Intel Corp.

CLee@SC9.INTEL.COM or CLee%SC9%SC.INTEL.COM@RELAY.CS.NET UUCP : {pur-ee,qantel,amdcad,oliveb,decwrl,hplabs}!intelca!mipos3!sc9!clee

🗡 California DMV Troubles

Master Of Darkness <clee@td2cad.intel.com> Sun, 30 Sep 90 16:42:30 PDT

The following was an article in the Sept 30, 1990 issue of "The Argus." One of the local papers in the SF Bay area.

DMV computer goof overbills car owners By Mark van de Kamp (staff writer)

Sham Dixit of Livermore was one of many California drivers who felt they were being asked to pay too much when they got notices this week to renew their motor vehicle registrations between now and November. And they were right. The state Department of Motor Vehicles admitted Friday that it had made a blunder which caused some drivers to be overbilled by hundreds, even thousands of dollars. In Dixit's case, he was asked to pay \$2,832 for his 1987 Nissan Sentra. It cost him \$166 to register the car last year. Likewise, three members of a Pleasanton family were overbilled by \$1,000 each.

The DMV does not know how many vehicle registrations are involved. There are 25 million registered vehicles in the state. The agency said the incorrect billing notices involve drivers whose vehicle registration was set to expire Nov. 16, 18 and 20. Most of the incorrect bills arrived in mailboxes Thursday and Friday. [...]

The problem surfaced late Thursday when DMV offices started receiving calls from motor vehicle owners asking why registration fees had changed significantly from the previously year, the agency said. "At first thought I'd made a mistake. Then I heard that the DMV screwed up. Boy, did they ever," Dixit said. "But I work with computers, so I know it must be a programming error. Computers are only as smart as the people who use them." [...]

Cecil Lee, Intel Corp.

[PGN Excerpting Service]

CLee@SC9.INTEL.COM or CLee%SC9%SC.INTEL.COM@RELAY.CS.NET UUCP : {pur-ee,qantel,amdcad,oliveb,decwrl,hplabs}!intelca!mipos3!sc9!clee

Report of Nat Semi clock chip flaw

Martyn Thomas <mct@praxis.co.uk> Thu, 4 Oct 90 12:38:35 BST

Electronics Times (4 Oct, front page) reports that National Semiconductor's real-time clock chip (part number MM58274B) "has a tendency to switch from a 24hr clock to a 12hr clock when subjected to electronic noise ...".

Two examples are given of problems allegedly caused by the chip.

"... the chip caused the time clock in a financial system to skip from Thursday to Saturday, leaving employees without paychecks".

"It has also caused problems for the United Nations Atomic Energy Agency which uses the chip in a televised security system for guarding nuclear fuel".

Martyn Thomas, Praxis (Software Engineers), 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

🗡 BA 747-400 Engine Failure

Martyn Thomas <mct@praxis.co.uk> Wed, 3 Oct 90 15:21:58 BST

Flight International (3-9 October) reports that a British Airways Boeing 747-400's No 1 engine electronic controls failed on takeoff at London Heathrow causing the engine to shut down.

The crew [two pilots, there is no flight engineer] reported the status message "engine controls" and asked their technical support staff, by radio, for advice. They were told "You've obviously lost control of that engine. It's a FADEC failure" [FADEC = Full Authority Digital Engine Controller].

BA says that the problem was a spurious signal from the electronic "thrust reverse resolver". If so, the early diagnosis of FADEC failure could be wrong. There has been a number of instances of spurious signals causing 747-400 engines to throttle back or shut down, according to Flight [This may be a reference to the earlier reports of spurious signals from flap and gear sensors, reported in an earlier RISKS].

Flight adds that FADEC failure is extremely unusual.

Martyn Thomas, Chairman, Praxis plc. Software Engineers. Tel: +44-225-444700. Email: mct@praxis.co.uk

✓ Equinox on the A320: Programme summary

1 Oct 1990 14:29:40-BST

Below is a summary of the Channel 4 (UK TV) programme on the A320 transmitted at 7pm Sunday 30 September. I took notes during the programme but I may have got some details wrong.

Equinox asked an independent air accident investigator named Ray Davis to examine the report on the Habsheim crash where an A320 being flown in a display made a slow pass over the runway and could not pull up in time to avoid the trees at the end of the airport. He made four major findings which were put to the Chief engineer (I think) at Airbus Industries.

- 1: A 4 second discrepancy between the Cockpit Voice Recorder, the Aircraft Data Recorder and the Tower Voice Recorder. Sorry but I cannot remember the Airbus reply to this.
- 2: There was no record of the impact with the trees in the flight data. This might be expected in (say) a collision with a mountain, but the recorders should have been able to operate until the aircraft disintegrated. Any crash which could be survived by all but three passengers should not have caused an abrupt stop in the flight data record. Again I cannot recall the Airbus reply.
- 3: The final seconds of the record showed forward acceleration. The airbus Chief Eng claimed that Davis had this graph upside down and a positive reading indicated deceleration. He also claimed that the deceleration was caused by the trees, and that Davis was incompetent if he did not know that this format was an international standard. Equinox stated that the international standard was for a forward acceleration to give a positive reading and that this was the one used by the A320. Airbus later stated that the CE had been referring to a French standard.
- 4: The final seconds of the record also showed the pilot giving full stick back but being overridden by the computer. The CE stated that this was the safety systems stopping the aircraft from stalling. Equinox said something about the Pilot manuals saying that at the indicated airspeed the aircraft should have been able to climb.

The possibility of an engine compressor stall leading to loss of power was discussed. According to Equinox this would lead to a small explosion (I assume this would be as unburnt fuel vapour was pushed out of the tailpipe) and a drop in power. A survivor and a ground witness stated that they had heard such explosions, but Airbus deny they occurred and point out that no such explosions are audible on the videotapes. An early transcript of the CVR did include the text "(boume) (boume)" (sp?). Airbus claim this is the sound of impact with trees.

About 30 seconds were devoted to a pilot employed by Airbus who had publicly

spoken out in support of Capt. Asseline (sp?) who was the pilot at Habsheim. This pilot claimed that 4 days later he was given an unscheduled medical examination and had his license withdrawn due to "mental instability".

The authenticity of the "black boxes" recovered from the crash was questioned. Officially the boxes are being held by a French court. Equinox was not allowed to film these, but a magistrate looked at a video alleged to be of the boxes immediately after being removed from the crash site and stated that if these were in fact the boxes from the A320 then something was very wrong. The implication was that the boxes delivered to the court were not the boxes recovered from the crash.

A video of the programme can be obtained by phoning +44 532 438283 ext. 4060 or 4075.

BTW, one of the interviewees had a box file labeled "RISKS" in the background. Perhaps he could fill in the holes in my report. Thanks.

Please note that this report is in no way connected with my employers. Paul.

Novel on corporate computer espionage

<pbrewer@urbana.mcd.mot.com> Tue, 02 Oct 90 10:07:13 CDT

Corporate espionage by computer is the subject of a new novel _The Fool's Run_ by John Camp. When plans for the latest fighter plane target acquisition hardware and software are stolen, a defense contractor decides that only by sabotaging the development work of a competitor can it be sure of being the only company in a position to demonstrate the system by the deadline. The company hires Mr. Kidd (artist, software designer, former commando) to invade the competitor's computers and disrupt their operations for a few weeks. They say:

the best way ... is through their computer systems--design systems, accounting systems, information systems, scheduling and materials. Altering them, destroying them, faking them out.

In the style of a classic caper novel, Kidd assembles a team including a burglar and a sleezy reporter and attacks the defense contractor, disrupting their operations from all sides.

The author handles the computer entry techniques well. There is only a small amount of "magic" involved, and most of that is performed in the background by "Bobby" (a former phone-phreak we meet only by way of a data link) who handles such things as telephone trace bypasses. The discussions of computer security techniques are right on target, and the supposed level of security at the target company is on par with what I've seen at several of the places I've worked. When it comes to the actual disruptions things get a little fuzzier, although not to the point that it fails to work as a novel.

In real life, most malicious computer attacks have been committed by disgruntled employees or former employees. Most computer viruses have been written by misguided enthusiasts. I haven't heard of this kind of attack against one company by another. That doesn't mean it hasn't happened, and it certainly doesn't mean that it won't happen. I fear, this book may give some people ideas.

Camp, John _The Fool's Run_ ISBN 0-451-16712-0 Signet \$4.95

Philip Brewer pbrewer@urbana.mcd.mot.com Motorola Urbana Design Center ...!uiucuxc!udc!pbrewer

✓ CERT Advisory - NeXT systems

<cert-advisory-request@cert.sei.cmu.edu> Tue, 2 Oct 90 14:57:03 -0400

CA-90:06 CERT Advisory October 2, 1990 NeXT's System Software

This message is to alert administrators of NeXT Computers of four potentially serious security problems.

The information contained in this message has been provided by David Besemer, NeXT Computer, Inc. The following describes the four security problems, NeXT's recommended solutions and the known system impact.

Problem #1 DESCRIPTION: On Release 1.0 and 1.0a a script exists in /usr/etc/restore0.9 that is a setuid shell script. The existence of this script is a potential security problem.

Problem #1 IMPACT: The script is only needed during the installation process and isn't needed for normal usage. It is possible for any logged in user to gain root access.

Problem #1 SOLUTION: NeXT owners running Release 1.0 or 1.0a should remove /usr/etc/restore0.9 from all disks. This file is installed by the "BuildDisk" application, so it should be removed from all systems built with the standard release disk, as well as from the standard release disk itself (which will prevent the file from being installed on systems built with the standard release disk in the future). You must be root to remove this script, and the command that will remove the script is the following:

/bin/rm /usr/etc/restore0.9

Problem #2 DESCRIPTION: On NeXT computers running Release 1.0 or 1.0a that also have publicly accessible printers, users can gain

extra permissions via a combination of bugs.

Problem #2 IMPACT: Computer intruders are able to exploit this security problem to gain access to the system. Intruders, local users and remote users are able to gain root access.

Problem #2 SOLUTION: NeXT computer owners running Release 1.0 or 1.0a should do two things to fix a potential security problem. First, the binary /usr/lib/NextPrinter/npd must be replaced with a more secure version. This more secure version of npd is available through your NeXT support center. Upon receiving a copy of the more secure npd, you must become root and install it in place of the old one in /usr/lib/NextPrinter/npd. The new npd binary needs to be installed with the same permission bits (6755) and owner (root) as the old npd binary. The commands to install the new npd binary are the following:

/bin/mv /usr/lib/NextPrinter/npd /usr/lib/NextPrinter/npd.old # /bin/mv newnpd /usr/lib/NextPrinter/npd (In the above command, "newnpd" is the npd binary that you obtained from your NeXT support center.) # /etc/chown root /usr/lib/NextPrinter/npd # /etc/chmod 6755 /usr/lib/NextPrinter/npd

The second half of the fix to this potential problem is to change the permissions of directories on the system that are currently owned and able to be written by group "wheel". The command that will remove write permission for directories owned and writable by group "wheel" is below. This command is all one line, and should be run as root.

find / -group wheel ! -type I -perm -20 ! -perm -2 -ls -exec chmod g-w {} \; -o -fstype nfs -prune

Problem #3 DESCRIPTION: On NeXT computers running any release of the system software, public access to the window server may be a potential security problem.

The default in Release 1.0 or 1.0a is correctly set so that public access to the window server is not available. It is possible, when upgrading from a prior release, that the old configuration files will be reused. These old configuration files could possibly enable public access to the window server.

Problem #3 IMPACT: This security problem will enable an intruder to gain access to the system.

Problem #3 SOLUTION: If public access isn't needed, it should be disabled.

- 1. Launch the Preferences application, which is located in /NextApps
- 2. Select the UNIX panel by pressing the button with the UNIX certificate on it.
- 3. If the box next to Public Window Server contains a check, click on

the box to remove the check.

Problem #4 DESCRIPTION: On NeXT computers running any release of the system software, the "BuildDisk" application is executable by all users.

Problem #4 IMPACT: Allows a user to gain root access.

Problem #4 SOLUTION: Change the permissions on the "BuildDisk" application allowing only root to execute it. This can be accomplished with the command:

chmod 4700 /NextApps/BuildDisk

To remove "BuildDisk" from the default icon dock for new users, do the following:

1. Create a new user account using the UserManager application.

- 2. Log into the machine as that new user.
- 3. Remove the BuildDisk application from the Application Dock by dragging it out.
- 4. Log out of the new account and log back in as root.
- 5. Copy the file in ~newuser/.NeXT/.dock to /usr/template/user/.NeXT/.dock (where ~newuser is the home directory of the new user account)
- Set the protections appropriately using the following command: # chmod 555 /usr/template/user/.NeXT/.dock
- 7. If you wish, with UserManager, remove the user account that you created in step 1.

In release 2.0, the BuildDisk application will prompt for the root password if it is run by a normal user.

CONTACT INFORMATION

For further questions, please contact your NeXT support center.

NeXT has also reported that these potential problems have been fixed in NeXT's Release 2.0, which will be available in November, 1990.

Thanks to Corey Satten and Scott Dickson for discovering, documenting, and helping resolve these problems.

Edward DeHart, Computer Emergency Response Team/Coordination Center (CERT/CC) Software Engineering Institute, Carnegie Mellon University Pittsburgh, PA 15213-3890 E-mail: cert@cert.sei.cmu.edu Telephone: 412-268-7090 24-hour hotline: CERT personnel answer 7:30a.m.-6:00p.m. EST, on call for emergencies other hours.

Past advisories and other information are available for anonymous ftp from cert.sei.cmu.edu (128.237.253.5).

Fair Information Principles

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com> Wed, 03 Oct 90 14:40:57 PDT

This is a summary of the Fair Information Principles, excerpted with permission from an e-mail message sent by Marc Rotenberg, directory of CPSR's Washington D.C. office and head of its Computers and Civil Liberties Project.

I thought RISKS readers might be interested.

FAIR INFORMATION PRINCIPLES

The Fair Information Principles were developed by a U.S. Government Study Committee in 1973, chaired by Willis Ware of the Rand Corporation. Shortly after the commission released its final report ("Records, Computers and the Rights of Citizens"), Congress passed comprehensive privacy legislation: the Privacy Act of 1974. Much of the privacy law that followed the Privacy Act (e.g., the Right to Financial Privacy Act, the Cable Policy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act) are based on the Fair Information Principles.

Many other countries follow the Fair Information Principles. Recently in Paris, European Data Protection commissioners recommended that the EC 92 charter include mandatory provisions for the enforcement of Fair Information Principles across all European countries.

These are the Principles:

1. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

2. There must be no personal data record-keeping systems whose very existence is secret.

3. There must be a way for a person to find out what information about the person is in a record and how it is used.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precaution to prevent misuses of the data.

Jeff Johnson, HP Labs

✓ Television rating (nee universal listening) device

Tim Wood at home <tim@axolotl.UUCP> Mon, 1 Oct 90 11:30:28 PDT

Found in the Oakland Tribune "Patents" column, Oct. 1, reprinted from The New York Times:

In search of a more accurate way to measure television and radio audiences, a small company in Chicago has patented a pocket-sized device that silently monitors and logs the programs a person listens to.

The battery-powered device is based on "acoustic matching." [this term is not precisely defined] ... [A] microphone senses sounds near the person being monitored and a microprocessor converts these sounds into a digital code.

... Users would place the monitoring devices on battery chargers when they go to bed. The battery charger would be connected to a telephone line, enabling the device to transmit the day's data to a central computer at the audience measurement company.

Hope all of your RISKS alarms are ringing as loudly as mine are. The frightening prospect of creation of libraries of users' private sounds comes to mind. As does the funny, if Machiavellian, image of public broadcasting of these sounds, a la the tryst between Majors Hoolihan and Burns in the movie "MASH."

This development is interesting in light of (what I see as) a duality in society's view of high tech of simultaneous infatuation and distrust. Hopefully the latter view will be applied to the new device. -TW

From under a Rock???

Ed Hall <edhall@rand.org> Thu, 04 Oct 90 11:56:40 PDT

I've been loosely following the various ``subliminal message" lawsuits which have been winding their way through the courts recently. These are product-liability suits alleging that subliminal messages in rock music have driven people to suicide. One such case, against British group Judas Priest, was recently dismissed. Another against Ozzy Osbourne is now pending.

There is a computer RISK here. According to today's Los Angeles Times:

... Sound Analyst Evans [a lecturer at Univ. of Nevada with masters degrees in physics and computer science] said she had spent about a month analyzing audio subliminal messages allegedly implanted on the "Blizzard of Oz" cassette using the same home-computer software package employed in the Judas Priest case. ... I can only guess at what this "home-computer software package" is. (If anyone has additional information about it, please let me know). One thing I'm sure of, however: it hardly affords an accurate model of human auditory perception (unless its author has managed to leapfrog what would no doubt be decades of neurophysiological research). Its use in court no doubt arises from the persisting association of The Computer with unchallengeable accuracy and authority.

I foresee nothing but trouble in the interaction between the notion of "subliminal messages" (whether auditory or visual) and the increasing capability for computers to perform extensive signal processing--whether that "processing" is meaningful or not. As the recent "Face on Mars" flap illustrates, people will see (or hear) just what they want to see (or hear), given the tools to create "evidence". Computers greatly enhance the power for self-delusion.

-Ed Hall, edhall@rand.org [Disclaimer: This all is my personal opinion ONLY.]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Bob Campbell <campbelr@grendel.cup.hp.com> Tue, 9 Oct 90 15:12:54 mdt

Deep inside the October 9th, 1990 San Jose Mercury News was this piece under the heading of "Unbelievably hot".

All sorts of explanations have been offered for record high temperatures across the country - the greenhouse effect, the growth of cities, even chance. But the National Weather Service is examining and additional theory: The thermometers were wrong. The service is studying the thermometer at issue, an electronic sensor called the Ho83.

Bob Campbell campbelr@hpda.cup.hp.com

Æ Equinox on A320 (UK Channel 4, Sun., 30th Sep)

Pete Mellor <pm@cs.city.ac.uk> Sat, 6 Oct 90 21:22:55 PDT

The 'Equinox' series of documentary programmes on science and technology on Channel 4 of UK TV was devoted to the Airbus A320 last Sunday (30th Sep., 7 pm). The one-hour film was made by Box Productions, main researcher Ben Hamilton.

A good summary of the programme has already appeared in <u>RISKS-10.47</u>, submitted by someone identified only as 'Paul'. He observed that:

> BTW, one of the interviewees had a box file labeled "RISKS" in the> background. Perhaps he could fill in the holes in my report.

That interviewee would have been Prof. Bev Littlewood, Director, Centre for Software Reliability, City University. We monitor RISKS at the Centre, and that box file does, in fact, contain printouts of the digests, so I can fill in the holes (although Paul hasn't left many for me to fill in!).

The programme updated an earlier programme on 6th Nov. 1989 and included much new material, in particular an independent analysis of transcripts of the data on the Digital Flight Data Recorder (DFDR) and Cockpit Voice Recorder (CVR) recovered after the crash at Mulhouse-Habsheim on 26th June 1988. This was done by Ray Davis, ex-Accident Investigation Bureau, UK Department of Trade and Industry, and now an independent consultant. He produced a written report which was submitted to Airbus Industrie (AI) for comment.

Davis concluded that:

- The flight control systems were not obeying the pilot's commands to lift the aircraft just prior to impact. (This supports the contention of the pilot, Michel Asseline, that he had requested 'nose up' and hadn't got it.)
- The DFDR recording stops 4 seconds *prior* to impact with the trees. (Davis added that, in his entire career, he had *never* come across a similar instantaneous stoppage of a recorder.)
- There is no indication of longitudinal deceleration, such as would have occurred due to impact with the trees, at the end of the recording.
- During the last part of the recordings, the DFDR and CVR are 4 seconds out of sync. (This is interesting in the light of the claim by AI that Asseline had not allowed sufficient time (7 sec.) for the engines to spool up to full power.)

Bernard Ziegler (Vice President, Engineering, Airbus Industrie) predictably dismissed Davis' report, describing it as 'pitiful'. He claimed that Davis had misunderstood the sign convention for acceleration/deceleration. In fact, according to the ARINC international conventions, Davis was right, and Ziegler was wrong. The point was put to Ziegler five times by the Equinox team, and each time he repeated this assertion. He then ended up with egg on his face
when his own organisation, AI, were obliged to retract, explaining that Ziegler had misunderstood, and had been using a French convention instead of the international one.

On one point, Ziegler appeared to accept Davis' findings, when he claimed that the safety systems were working to prevent a stall (i.e., overriding the pilot's request for 'nose up'). Asseline claims that the aircraft had sufficient speed and power to clear the trees without stall.

Air France, and the Bureau Enquetes Accidents who produced the original accident report, refused to be interviewed. The copilot at Mulhouse, Jaques Mazieres, is still flying for Air France, and so also not available.

Davis stated that there must now be another enquiry, and that this must take account of the improper pressure being applied in certain quarters. (Asseline has received threats; Norbert Jaquet, an Air France pilot who spoke out in Asseline's support, was suspended from duty and had his licence withdrawn on the grounds of 'mental instability'.)

Even the authenticity of the recorders was called into question. The boxes were filmed last year by Equinox in the boot of the car of the director of the DGAC at the scene of the crash, and a French journalist also saw them. According to Asseline, those produced at the enquiry do not resemble these. The original investigating magistrate at Mulhouse, Germain Sengelin, said that there was a 'problem in relation to justice'. (The present magistrate has obtained an independent report on the evidence used by the commission of enquiry, which also concludes that there is serious doubt over the authenticity of the recorders and the readouts made from them.)

The programme went on to consider the crash of the A320 at Bangalore. A pilot was interviewed saying that it was virtually unknown for an aircraft to lose height in such a way in clear conditions on a landing approach. Air India has now grounded all its A320s at enormous cost. Prince Dandonda (sorry - no note of his job title) was interviewed saying that they have never seen this amount of failures in an aircraft. One example was of a bird strike on the windscreen resulting in a shut-down of three display computers, and causing the system to shut down one engine.

There was an interesting example of Ziegler's logic concerning the Bangalore crash: we know it wasn't bad weather, we know it wasn't bird strike, it *can't* have been the aircraft systems, *therefore* it *must* have been pilot error.

Davis' view is that a crash should be ascribed to 'pilot error' *only* where there is positive proof. 'If you don't fully establish the cause of an accident, then that accident will happen again.'

The programme concluded that, in the meantime, 'Air France and Airbus Industrie must live with the fact that there is a question mark over the safety of the A320.'

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET) [My humblest apologies to Paul. The From: field was deleted instead of the To: field and paul accidentally remained anonymous. PGN]

🗡 Ada and multitasking

<KRISTIA@ESTEC.BITNET> Mon, 08 Oct 90 10:28:12 CET

Re: "Ada's fundamental language structures build reliable systems", article by Benjamin M.Brosgol in EDN, September 3, 1990, international edition.

The article starts:

- > Ada's principal goals are program reliability, readability, efficiency, and
- > portability. Many real-time application programs, such as those used in
- > avionics, telecommunications, and manufacturing, need these features
- > because of the large, complex, and long-lived pieces of software involved.

The author then describes several features of the Ada language, such as data typing, separate compilation units, and concurrent tasks.

The RISKy bit comes in the discussion of task priorities. It becomes clear that the Ada language falls short of completely and unambiguously defining how the task scheduler must deal with the priority issue, and that some freedom is left to the implementor in this area.

The following quotes from the article give a flavour of the problem:

- > In addition, when a select statement has several open alternatives,
- > implementations need not take priorities into account when deciding which
- > one to accept. Instead, for example, they can take fairness criteria into
- > account.

and

- > Ada language implementations can solve the problem of nondeterminism when
- > there are several open alternatives by providing directly or letting you
- > dictate the use of task priorities.

The author does not seem to realize the contradiction between the *reliability* and *portability* quoted as features of Ada on one hand, and the lack of definition of crucial features on the other.

Stated briefly, the RISK that I want to address is:

A language which boasts high portability and reliability includes features which mean that there is no guarantee that a program will work the same way if ported to another compiler and/or run-time environment.

Even worse:

The potential differences are are hidden deeply below the "visible surface" of the program, and are implicit in nature. This means that the program will probably compile and link after being ported. It is also likely to show a very similar behaviour to the original so that a superficial testing may not reveal any problems. But problems may still be lurking in the dark corners of

infrequent (but perfectly possible and legal) sequences of events. For example, superficial validation testing is likely to test mainly rather "quiet" modes with stimuli applied one at a time. But scheduler-related problems are more likely to show up when the software is very "busy", e.g. due to an abnormal or emergency situation creating many stimuli, such as alarms.

A further RISK is that a language which is claimed to be designed for portability may encourage reduction in (costly and time-consuming) in-depth validation testing after porting the software to a different environment.

In fact, the real RISK is maybe not that Ada has these shortcomings. The RISK, to my opinion, is that Ada, in spite of its shortcomings, claims to be highly portable and reliable.

Does anybody have any experience (good or bad) in porting Ada programs, in particular real-time programs?

Erling Kristiansen, European Space Research and Technology Centre, Noordwijk, The Netherlands. Usual disclaimers apply.

Ke: Arbitration Myths (Peter Denning, <u>RISKS-10.42</u>)

<cosell@BBN.COM> Fri, 5 Oct 90 12:27:25 EDT

}As Peter observes, the only way to build a computer that is safe from
}"arbitration failure" is by making choice 1, which means that the computer must
}turn off its clock while waiting for an arbiter to decide. Note that the
}computer can't keep its clock ticking while waiting for the arbiter to make up
}its mind, since it would then require another arbiter to decide within the
}current clock cycle whether or not the first arbiter had made up its mind. I
}know of no computer that turns off its clock in this way.

The DEC PDP-6 line worked this way. It was a fully asynchronous CPU and would happily wait for as long as it took for an operation to complete. At MIT they had one word of memory implemented out of elevator relays [2 second read time or the like]. The 'flow chart' for how long a simple 'add' instruction took took up two pages in the manual [including delays for waiting for the memory, delays for carry propagation, etc].

/Bernie\

California DMV and Italian publicity

A Product of Society <jon@pacbell.UUCP> Sat, 06 Oct 90 15:39:06 PDT

I have nothing against Italians, only against ignorant Public Relations people.

A month ago my mom got a letter in the mail, from the California DMV. On

behalf of the Italian community, it said, (who had recently launched a PR stunt against anti-italian bumber stickers and etc) she would have to change her license plate. Her plate read "WOPER1", comming from a feminist's word "WOman PERson". The '1' was there because the "lisence plate bible" reported that someone already had WOPER.

The Italian PR guy had the DMV search their computers for any string containing WOP. There's a risk here, no doubt: My mom's plate had *nothing* to do with Italians, and there are plenty of words that grep might pick up, all containing WOP.

My mom wrote an extremely formal letter (she's an attorney, after all, and that's good for *something* :) to the DMV, and they apologized over the phone. They would change the plate, however, to "WO PER", with half a space, to distinguish this word from any anti-Italian slang. They also reported that the first person having "WOPER" no longer had the plate, and "WOPER" was available for use.

The plate arrived last week. It read "WOPER". Nice job on behalf of the DMV. The bill for the plate read \$1,200. There's a connection here...

The *actual* bill was \$108.xx, because of the recent computer foul up, posted in the last issue.

Should agencies like the DMV be allowed to just 'grep' a database on behalf of a PR stunt for *any* phrase containing "WOP"? Something is wrong here. Next thing you know, colleges will be scanning their applications for last names ending in "ez" to fill some quota of Mexican students. Mexicans aren't the *only* people whose last names might end in --ez, just as WOP-- isn't *always* a derogatory slang against Italians!

Computers are becomming more useful to the tools of prejudice.

Jon ..?\$!..ames!pacbell!sactoh0!vector0!jon vector0!jon@sactoh0.SAC.CA.US

✓ Government routinely ignores Privacy Act

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Tue, 9 Oct 90 15:01:14 PDT

Excerpted from Gov't Computer News, 10/1/90:

Agencies violated the Privacy Act 292 times last year by failing to notify the public about a third of their largest personal record systems . . . The report by GAO's Information Management and Technology Division, Computers and Privacy said many agencies ignored the Privacy Act's publication requirements and did not issue Federal Register notices for 35 percent of their personal records systems . . .

The Defense Department reproted the most systems covered by the law with 360, followed by the the departments of Health and Human Services with 210, Justice with 169,, and Agriculture with 87. However, agencies published notices for only 535 systems . . . 46 agencies told they participated in computer matches . . . The report said 4.32 million matches, 78% of the total, were done for law enforcement purposes. Another 16,245 were for tax purposes, and 10,028 involved queries on delinquent payments. The Drug Enforcement Administration and Farmers Home Administration accounted for 97% of all matches.

I observe that many federal criminal databases are not even covered by the Privacy Act's provisions, and that computer matching of government databases was supposedly prohibited by the Privacy Act. [CJ]

computer sound editors are appropriate technology, not deceipt

"David A. Honig" <honig@ICS.UCI.EDU> Mon, 08 Oct 90 16:43:44 -0700

In <u>RISKS-10.47</u>, Ed Hall <edhall@rand.org> writes: > There is a computer RISK here. According to today's Los Angeles Times:

... Sound Analyst Evans [a lecturer at Univ. of Nevada with masters degrees in physics and computer science] said she had spent about a month analyzing audio subliminal messages allegedly implanted on the "Blizzard of Oz" cassette using the same home-computer software package employed in the Judas Priest case. ...

>I can only guess at what this "home-computer software package" is. (If >anyone has additional information about it, please let me know).

There are several programs that allow one to aquire, process, and play-back sound on various PCs. The analyst in this case would be most interested in playing sound back time-reversed, perhaps with some equalization afterwards. She would try different transforms exhaustively to see if she could hear any nasties.

This of course is identical to what one can do with a magnetic tape player, or a phonograph if one is willing to trash the disk and needle.

I would expect that the expert witness would have to explain her methods and tools to the court. I see nothing even implicitly deceitful in using a Macintosh to play sound backwards...

He continues:

>thing I'm sure of, however: it hardly affords an accurate model of human >auditory perception (unless its author has managed to leapfrog what >would no doubt be decades of neurophysiological research).

Huh? The analyst is just playing the sound back, not doing *pattern-matching* for curses in latin backwards...

>Its use in court no doubt arises from the persisting association of

>The Computer with unchallengeable accuracy and authority.

Its use in court is a result of the expert sound analyst using up to date tools. If there were sounds encoded in the music, digital signal processing techniques are better tools to use than analog ones.

The whole business is the pathetic process of ill families trying to put the blame for their kids' suicides on the Evils of Rock and Roll (tm)...

&isclaimer: I don't listen to the stuff...>

✓ Operation Sun Devil invades the InterNet?

"Jonathan I. Kamens" <jik@pit-manager.MIT.EDU> Mon, 8 Oct 90 05:50:04 -0400

The message by Ed Luke (who is, incidentally, the SysOp of the MARS BBS discussed in it) is, indeed, a hoax.

For more information about it, see the article entitled "MARS BBS Sting a Prank" in Issue #2.06 of the Computer Underground Digest (available in alt.society.cu-digest for those of you who read news and whose feed includes that newsgroup). The article does a good job discussing the risks made clear by this "joke".

The article claims that the prank was "not malicious" and "not intended to be deceptive". Unfortunately, in the real world, there is often a gap between what is intended and what actually occurs. Many people *were* deceived by his story, and I'm sure that it caused some people quite a bit of worry about the possibility that Operation Sun-Devil might be coming after them next.

I do not think Mr. Luke used very good judgment at all when he wrote his "prank".

Jonathan Kamens, MIT Project Athena

✓ Loving Little Egypt - phone freaks

Dick Karpinski <dick@ccnext.ucsf.edu> Fri, 5 Oct 90 15:34:11 PDT

In Loving Little Egypt (ISBN 0 14 00.9331 1), the protagonist is a weak sighted boy who discovers vulnerabilities in the in-band signalling of the early dial telephone network. This delightful tale includes episodes of interaction with Bell, Edison, Tesla and others in a quest to improve the security of the phone system. Comparisons with Morris come readily to mind. The interactions among the blind phone freaks also invite comparison with the Whole Earth Review article on the facts and people involved by the Secret Service in Operation Sun Devil. This book uses science and technology as major plot elements, which seems to be a major problem for folks like the operatives in Sun Devil. The risks involved here range from technical vulnerabilities to serious loss of freedoms due to heavy handed tactics by uncomprehending agents of law enforcement organizations.

Dick

CERT Advisory Update - NeXT Systems (See <u>RISKS-10.47</u>.)

<cert-advisory-request@cert.sei.cmu.edu> Fri, 5 Oct 90 11:52:48 -0400

This message is an update of the October 2, 1990 CERT Advisory (CA-90:06) "NeXT's System Software". There is one correction and an update that you should be aware of.

For Problem #2 SOLUTION, the following line has been added:

/etc/chmod 440 /usr/lib/NextPrinter/npd.old

This will disable the old printer program.

NeXT is also making the new printer program, npd, available electronically via anonymous ftp for Internet sites. The archives sites are:

nova.cc.purdue.edu umd5.umd.edu cs.orst.edu

In addition, NeXT has asked the CERT to announce that if anyone cannot get it from the archives, NeXT Technical Support can provide it. Requests should go to:

ask_next@NeXT.COM [...!next!ask_next]

Ed DeHart, Computer Emergency Response Team



Search RISKS using swish-e

Report problems with the web pages to the maintainer



×

Wed, 10 Oct 90 20:49:32 -0700 From: jdudeck@polyslo.CalPoly.EDU (John R.

Phone lines - including the 911 emergency number - were dead throughout San Luis Obispo [California] for thirty minutes Tuesday night [Oct 9, 1990].

The interruption, which affected 30,000 customers, occurred at 10:15 p.m. and affected virtually all phone lines in the city, said Jim Bower, Pacific Bell's Central Coast area manager.

Bower said the interruption was caused by a computer programming error made by a Pacific Bell employee. "We were putting in a new program and an error was made," he said. "We were responsible for the error and corrected it as soon as we could."

The error also caused phone lines at the Sheriff's department, including the 911 number, to go dead for 30 minutes, said Sheriff's Sgt. Scott Thompson. The disruption didn't cause any serious problems, he said.

- San Luis Obispo Telegram Tribune, Oct. 10, 1990, p. A-5

John Dudeck, jdudeck@Polyslo.CalPoly.Edu ESL: 62013975 Tel: 805-545-9549

×

Thu, 11 Oct 90 15:08:40 CST From: Ed McGuire

Our organization has been playing the game of Phone Tag a lot recently. We reasoned that, if the other player could leave a voice message for us instead of asking a receptionist to have us call them back, we would win the game more often. (Not to mention improve our response to our customers.) Accordingly, we installed telephone answering machines for several people, including myself, on the desks next to the telephones. The telephones are just the visible part of the campus' fancy private branch exchange (PBX).

The PBX was insulted when I installed my machine. Accordingly, when one of our secretaries tried to call me, it rang my phone only two times while it rang in the callers ear four times, then "forwarded on no answer." When the secretary answered her phone, she was talking to herself.

So I told my machine to answer on two rings. Then I found out that my machine has a bad attitude.

For two days it left me "1 message waiting" but there was nothing on the tape. I discovered that it had been telling people to leave their name, company and phone, then hanging up on them. This was because I had mistakenly moved the wrong one of two identical switches on the side to fix the earlier problem.

Today I caught my machine cheating at Phone Tag.

I started the game by making a call to a person in our Inventory Department. The line was busy, so I tagged her by instructing our telephone system to call me back when she hung up. YOU'RE IT.

A few minutes later I left my desk on a short errand. And while I was gone, she hung up and my phone rang. But now my machine saw its opportunity! It answered the call, apologized to her for my absence and instructed her to leave her name, company and phone. YOU'RE IT.

The message I received on the machine made it clear that this was breaking the rules of the game.

* * *

Fortunately, this last event never actually happened. I realized the risk I was taking due to the interaction of two Phone Tag technologies just before I left my office. A colleague and I simply tested and verified the correctness

of my scenario.

Ed

Miscovery misprogrammed

Fernando Pereira <pereira@research.mercury.nj.att.com> Wed, 10 Oct 90 22:30:10 EDT

Summary of story by AP Science Writer Lee Siegel ``Wrong Computer Instructions Were Given to Discovery Before Liftoff''.

According to Discovery flight director Milt Heflin, the shuttle was launched with incorrect instructions on how to operate some of its programs. The error was discovered by the shuttle crew about one hour into the mission, and was quickly corrected. NASA claims that automatic safeguards would have prevent any ill effects even if the crew had not noticed the error on a display. The error was made before the launch and discovered when the crew was switching the shuttle computers from launch to orbital operations. The switching procedure involves shutting down computers 3 and 5, while computers 1 and 2 carry on normal operations, and computer 4 monitors the shuttle's ``vital signs'' [I'm just following the article on this, I don't know whether it is accurate]. However, the crew noticed that the instructions for computer 4 were in fact those intended for computer 2. Heflin stated that the problem is considered serious because the ground pre-launch procedures failed to catch it.

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

X Airliner story

Gene Spafford <spaf@cs.purdue.edu> Wed, 10 Oct 90 12:25:11 EST

A few months ago, I told a friend about the various stories I had read here and elsewhere about the A320. The subject came up when I explained why I would never again fly Northwest Airlines (they bought a bunch of A320s for domestic use).

He just recently sent me this mail:

<> From: RIch EPstein <@VM.CC.PURDUE.EDU:REPSTEIN@GWUVM><> To: Spaf <spaf><> Date: Tue, 09 Oct 90 16:13:44 EDT<> I just came back from the IEEE Visual Languages WOrkshop, which<> I thoroughly enjoyed. However, I thought you would find my<> air horror story of interest:<> The conference was in Skokie, ILL, so I had to fly in and out<> of O'Hare. We had a slight mishap on the plane on the way back<> to Dulles. Heavy rains leaked into the plane and knocked out

<> the transponders and the auto-pilot computer. About 15 minutes <> into the flight the pilot announced that we had to return to <> O'Hare because the air traffic controllers couldn't "pick us <> up". In other words, we were invisible, in the clouds, at <> O'Hare. According to an Air Force ROTC student here at GW <> the pilot meant this literally. Radar picks up aircraft by <> means of the signal sent out by the transponders. <> We flew around in the clouds for 15 more minutes. We landed

<> with all sorts of emergency vehicles on the runway. Then we <> waited for almost three hours until they finally replaced <> the transponders and computer and we left Chicago on the <> same plane (which I didn't like too much). <>

<> The pilot got on the p.a. system after we were successfully
<> on our way to Dulles and he made an interesting remark. He
<> said that this was a good plane because it had "stainless
<> steel aeronautical control cables", a reference to the fact
<> that an Airbus would probably have been disabled completely
<> in a similar circumstance. I have no doubt that the pilot
<> was referring to the Airbus when he made this remark.

I wrote asking his permission to send this on to Risks, and in his reply, he said:

<> By the way, I think the ground crew at O'Hare might have been <> negligent in my airline incident. When we entered the airplane <> water was LITERALLY POURING INTO THE AIRCRAFT at the door to <> the airplane. Passengers had to JUMP THROUGH a sheet of water, <> a thin veil, maybe 1/4" thick, but continuous. The water was <> coming in from the top of the door and onto the floor of <> the airplane. Obviously, the water went from there into the <> underbelly of the craft. The reason for this was that the <> airport walkway was not meeting the fuselage correctly.

* An IBM interface glitch & RISKS masthead FTP instructions

Lorenzo Strigini <TRIGINI@ICNUCEVM.CNUCE.CNR.IT> Mon, 08 Oct 90 09:49:54 MET

Just to signal another minor problem similar to that of truncation to 80 columns: After several unsuccessful attempts to follow the masthead instructions for FTPing RISKS issues, I discovered this morning that my IBM3278 emulator eats square brackets. CRVAX runs VMS, I guess, but I hadn't used such a system for years: only when I moved my attempts to a Unix machine did I realize why I could not cd to the risks directory.

The 3278 keyboards don't have square brackets, but square brackets entered through an emulator are stored as escape sequences. ASCII square brackets that exist in mailed of FTPed files are stored as such, and displayed as blank spaces.

and here are a few left square brackets embedded in a series of dashes:

and a few right brackets:

Amazing... I thought this was worth signalling in case you receive requests for help from other IBM users.

Lorenzo

Lorenzo Strigini, IEI del CNR, Via Santa Maria 46 I-56126 Pisa ITALY Tel: +39-50-553159 ; Fax: +39-50-554342 ; strigini@icnucevm.bitnet

[Lorenzo and RISKSers, I have long been annoyed at the miserable VAX command "cd sys\$user2:[risks]" to get the anonymous FTPer into the RISKS directory. In response to Lorenzo's message, SRI's CRVAX wizard Ray Curiel, at Steve Milunovic's request, has provided a terse alias: "cd risks:". Upper/lower case does not matter, but the colon does. HooRAY! Thanks. I changed the masthead. Now you don't need to escape from the colonease? PGN]

Automobile Computer RISKS - A Real Life Experience

Marc Lewert <marc@frederic.octel.com> Wed, 10 Oct 90 12:58:25 PDT

With all of the discussion on the risks of computerized and/or electronic controls in Aircraft, one should not overlook the fact that there could be more down to earth (pun intended) risks along the same lines.

One of our cars has a computer, and various other electronic sensors that control the engine. A couple of years back, shortly after we bought the car, it started intermittently losing power. Not too much trouble on city streets, but on the freeway, it was downright dangerous.

The symptom was that the car's engine would drop to idle speed, and would not speed up, not matter what we did with the gas pedal. It could be reset by turning off, and restarting the engine.

We had brought the car in several times, but the dealership could not find the problem.

Then came the fateful day...My wife was driving the car when the engine dropped to idle at the merge of two freeways, and she was in slow lane of one freeway that merged with the fast lane of the other...I was not happy when I got the call (I told her to call the dealership to come get the car!).

Somehow she was talked into driving the car to the dealership, when the same problem occured. This time, though, it occured in front of a truck hauling an oversized load in the slow lane of the freeway. If there had not been an offramp and a truck driver that was on his toes, we might be talking about my wife in the past tense at this point.

The eventual problem was an intermittent failure of a sensor in the air intake system. The computer responded by cutting down the fuel flow to its minimum setting.

I just wonder how many of these types of problems exist out in the world, and if anyone had been killed by them. All in all, everyone was very lucky... This Time.

Re: BA 747-400 Engine Failure (Thomas, <u>RISKS-10.47</u>)

The Polymath <hollombe@ttidca.tti.com> 11 Oct 90 01:49:21 GMT

}... It's a FADEC failure" [FADEC = Full Authority Digital Engine Controller].
 }... There has been a number of instances of spurious signals causing
 }747-400 engines to throttle back or shut down, according to Flight ...

This begins to sound a bit like the discussion of electronic vs. mechanical rail line switching controls.

I earned my Airframe & Powerplant mechanic's license (A&P) nearly 25 years ago (when pilots were made of iron and planes were made of wood ... but I digress (-:). At that time, jet engine controls were almost entirely mechanical, consisting of amazingly complex blocks of pneumatic and hydraulic sensors and actuators. Each engine had a main controller and a backup, "get you down alive" controller that provided just enough control to keep the engine running if the main failed.

Has the concept of such backups been lost in the rush to computerize?

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

Ke: Equinox on A320 (Pete Mellor, <u>RISKS-10.48</u>)

<ken@minster.york.ac.uk> 11 Oct 1990 18:09:03 GMT

>The programme went on to consider the crash of the A320 at Bangalore. A pilot >was interviewed saying that it was virtually unknown for an aircraft to lose >height in such a way in clear conditions on a landing approach.

We know that the Bangalore crash _was_ pilot error. Both the `back box' and the cockpit voice recorder indicate that the pilots were to blame. Flight International has given a good account of this, including the CVR transcript. The captain left the aircraft in idle descent mode and flew into the ground. The aircraft warned the pilots (both visually and aurally), but they ignored the warnings. Equinox chose not to report this (the rest of the programme seemed very convincing).

A lot of people have a lot of axes to grind over Airbus Industrie, and

receiving totally impartial and accurate information is almost impossible. Listen to Boeing and you hear that the A320 is a death-trap. Listen to Aerospatiale and you hear supreme confidence. Watch TV programmes and you see sensationalism.

Ken Tindell, Computer Science Dept., York University YO1 5DD, UK Tel.: +44-904-433244 UUCP: ...!mcsun!ukc!minster!ken

K Re: Equinox on A320 (UK Channel 4, Sun., 30th Sep)

<henry@zoo.toronto.edu> Wed, 10 Oct 90 12:39:31 EDT

>- The DFDR recording stops 4 seconds *prior* to impact with the trees. (Davis

> added that, in his entire career, he had *never* come across a similar

> instantaneous stoppage of a recorder.)

Is it possible that Davis is not familiar with *digital* flight recorders? I've seen some commentary on such an issue in the aviation press recently: the underlying problem is that some (all?) digital flight recorders buffer incoming data in semiconductor memory, which loses its contents on power failure. The airworthiness authorities are starting to be seriously displeased with the potential for loss of crucial data, and there are mutterings about requiring non-volatile memory.

I don't know for sure that this accounts for the above claim, but it certainly sounds like the right sort of symptoms.

(Would a simple explanation like this go unconsidered? Quite possibly, especially in the context of a media story whose basic slant is "dirty work at the crossroads". As I've commented before, there is a problem with the A320 business in that almost all participants have axes to grind and it is very difficult to get a balanced view. The media are not exempt from this, since sensation sells and boring truth doesn't.)

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

Ke: Ada and multitasking (Kristiansen, <u>RISKS-10.48</u>)

Stephen Tihor <IHOR@ACFcluster.NYU.EDU> Wed, 10 Oct 1990 17:03:25 EDT

The areas left to the implementer were left that way due to disagreements on the proper and useful choices. All such options must be fully specified in mandatory sections of the Ada reference manual.

The general phrase I remember being used whenever such items were discussed is that the market will select among conforming compilers.

In hindsight it might have been better to add some language clauses that allow you to specific or explicitly leave unspecified the tasking priority

requirements.

On the other hand many people believe that the ADA tasking model, while interesting, is not general enough to begin with.

Re: Ada and multitasking

<henry@zoo.toronto.edu> Wed, 10 Oct 90 12:59:53 EDT

> The author does not seem to realize the contradiction between the
 > *reliability* and *portability* quoted as features of Ada on one hand, and
 > the lack of definition of crucial features on the other.

There is no inherent contradiction here, unless "reliability" and "portability" are taken to include the phrase "guaranteed or your money back". (Mind you, some of the Ada enthusiasts essentially do claim this.) "Reliability" and "portability" are not absolutes, especially in a language constrained to be implemented efficiently on current machines. If such constraints mean that a particular feature is not completely defined, this just means that reliable/portable programs must avoid depending on it. This does require competent programmers, however, and one gets the impression that some of Ada's big backers hoped that their wonderful language would do away with the need for competence. After all, it's much easier to run a test suite through a compiler than to decide whether a programmer is competent.

The C community regularly sees broadsides on the subject, with ignorant people claiming that the large number of "implementation defined" or even "undefined" items in ANSI C implies that C programs cannot possibly be portable or reliable. Not so; these are just indications of where the programmer must avoid depending on implementation-dependent behavior. (There is room for legitimate debate about whether C expects too much from its programmers, but that is a different issue. Portable, reliable C code is verifiably possible.) C gets more of this than Ada, because C is a rather unforgiving language meant for people who know what they are doing, but almost any efficient language will run into similar issues.

To draw an analogy from more traditional engineering, the basic art of designing circuits with transistors is organizing things so that the characteristics of individual transistors do not affect the outputs much. Transistor characteristics are quite variable, especially if you want the transistors to be cheap. This does not make it impossible to design transistor circuits with predictable properties. It merely requires that designers take care to use circuits that allow for the variability and cancel it out.

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Pete Mellor <pm@cs.city.ac.uk> Mon, 15 Oct 90 17:25:56 PDT

Excerpts from The Independent on Sunday, 14 Oct 1990:

Headline: "Hackers blackmail five banks"

Subhead: "Mysterious computer experts demand money to reveal how they penetrated sophisticated security"

By-line: Richard Thomson

"At least four British clearing banks and one merchant bank in the City are being blackmailed by a mysterious group of computer hackers who have broken into their central computer systems over the last six months. These breaches of computer security may be the largest and most sophisticated yet among British banks. The electronic break-ins, which began last May, could cause chaos for the banks involved. Once inside their systems, the hackers could steal information or indulge in sabotage, such as planting false data or damaging complex computer programs. It is unlikely, however, that they would be able to steal money.

So far, the hackers have contented themselves with demanding substantial sums of money in return for showing the banks how their systems were penetrated. None of the banks has yet paid.

[Stuff omitted]

One computer expert described their level of expertise as "truly frightening". They are not believed to have links with organised crime, which has become heavily involved in computer hacking in the US over the last two to three years. [Any comments?? - PM]

It is a severe embarrasment for the banking community which is frightened that public awareness of the security breach could undermine public confidence. As a result, they have not called in the police but some have hired a firm of private investigators, Network Security Management, which is owned by Hambros Bank and specialises in computer fraud. It is common for banks not to report fraud and security failures to the police for fear of damaging publicity.

All the banks approached either denied that they were victims of the blackmail attempt or refused to comment.

The hunt for the hackers is being led by David Price, managing director of NSM, who confirmed his firm was investigating security breaches at five British banks. "I am confident of success in catching the hackers." he said.

[Stuff omitted]

Security measures were tightened after a large computer fraud at a leading City bank three years ago. Although the bank involved was never named, it is understood the money was never recovered. [Anyone got the details?? - PM]

[Stuff omitted]

According to an expert, who recently advised one of the big four clearers on its computer systems, there are few people who understand the bank's system well enough even to detect a break-in.

[Stuff omitted]

According to some reputable UK and US estimates, up to 5 per cent of the gross national product of western economies disappears in fraud. Experts say that the senior managers of many companies simply do not appreciate the need for tight security.

[Stuff about the Computer Misuse Act omitted]"

---- End of extract ----

Just how "sophisticated" banks' computer security is can be judged from a conversation I had last Saturday night in the pub with an acquaintance who manages the local branch of a chain of off-licences (liquor stores).

He had just finished entering his orders onto his PC, which communicates remotely with the firm's main warehouse in Dartmouth (I think). He told me that he entered the normal 5-digit code to send in his completed order, and was amazed to find displayed on his screen the credit card transaction records from Barclays' Bank in South Yorkshire, with full details: names, account numbers and amounts.

Feeling thoroughly confused, he switched off the machine and went to bed. When he checked the next day, he found that his order *had* been correctly received.

Obviously just a one-off incident that need not affect public confidence!

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

[Also reported by Sanford Sherizen <0003965782@mcimail.com>]

🗡 Equinox on A320

Robert Dorsett <rdd@rascal.ics.utexas.edu> Fri, 12 Oct 90 23:59:54 CDT

<>The programme went on to consider the crash of the A320 at Bangalore. A pilot
<>was interviewed saying that it was virtually unknown for an aircraft to lose
<>height in such a way in clear conditions on a landing approach.

>

>We know that the Bangalore crash _was_ pilot error. Both the `back box' >and the cockpit voice recorder indicate that the pilots were to blame. >Flight International has given a good account of this

On the other hand, Flight International has been extremely close to Airbus throughout the development of the aircraft. While I like the magazine, it is also a proponent of Euro-oriented industry, and has been very careful not to say anything too damaging about the airplane--and has certainly not given detailed consideration to the voluminous controversial issues which surround many aspects of the aircraft.

At the risk of sounding like a broken record, I suggest the following: "pilot error" is an unacceptable answer. In clear, stable conditions, with an (apparently) operational airplane, one just doesn't go around crashing airplanes. "Pilot error" might be acceptable if, say, one reverses a holding pattern and flies into a mountain in clouds, but Bangalore (and Habsheim) smacks of a systemic error of some sort. What could it be? Let's see:

- the airlines' hiring and qualification mechanisms (ab initio).
- the training mechanism (computer-*based* training, supplied by Airbus)
- the overall *philosophy* of the flight deck design (Airbus)

- individual components of flight deck design (altimeter design, etc)

- support system problems (FADEC unresponsiveness, ignoring commands which put the airplane out of the computed "safe" envelope)

The emphasis on RISKS has long been on the last category: concerns on hardware and software failure, common sources of failure, etc.

>The captain left the aircraft in idle descent mode and >flew into the ground. The aircraft warned the pilots (both visually and >aurally), but they ignored the warnings. Equinox chose not to report >this (the rest of the programme seemed very convincing).

This supports the systemic view. In my experience on an A320 simulator (reported on sci.aeronautics about five weeks ago), I noted that there were way too many alerts. There are two types: warnings and cautions. They both have the same chime, but illuminate different lights. They often deal with uttelry trivial situations, but require the pilot to drop what he's doing and sort through the ECAM displays to figure out whether to spend any MORE time on it. In many cases, the computer's already taken care of cautions, so, "why worry?"

Apart from too many alerts, ground-proximity warning systems have a poor reputation in the airline industry as a whole: false warnings at cruising altitude, warnings during properly-conducted approaches, etc. These have been with us for nearly 20 years; crew reluctance to pay attention to them have resulted in several other airliner crashes (although it's undeniable that the systems have also saved lives).

Lastly, there has *always* been a tendency in the airline industry to make unworkable or poor designs work (e.g., Comet, DC-10). Given a poorly designed cockpit, the tendency is to attempt to train around any defects. Ditto with a bad airplane. This *suppresses* the consequences of systemic error, but by no means *eliminates* it. When "pilot error" happens in this environment, all too often the operator is castigated, while the circumstances which produce the error is ignored.

I suggest (again) that the way the airplane interacts with the pilot is at LEAST as important as component-wise reliability. Just because the machine works does not mean that the machine's *design* is satisfactory for human operation. This is a consideration that will become increasingly important with all aspects of automation, and needs to be addressed in this forum. This has nothing to do with lawsuits, sensationalism, or PR-types. It has to do with saving lives, and preserving the capability of the human component of safety-critical systems to do its role properly.

End of diatribe.

Robert Dorsett UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

Ke: A320s and Northwest Airlines (Epstein/Spaf, <u>RISKS-10.49</u>)

<ckd@cs.bu.edu>

Sat, 13 Oct 90 11:07:01 -0400

spaf> Gene Spafford <spaf@cs.purdue.edu> said: spaf> A few months ago, I told a friend about the various stories I spaf> had read here and elsewhere about the A320. The subject came up spaf> when I explained why I would never again fly Northwest Airlines spaf> (they bought a bunch of A320s for domestic use).

I've seen a few of them; never flown on 'em, though (hey, *I* read RISKS!). My policy still is to always check the aircraft type when making reservations.

My big "Northwest A320 story" is of a time I was flying from Seattle to Boston, with a stop in Detroit. There was a DC-10 at Detroit with a gate hold for maintenance (hydraulics problems, I believe) and they swapped our aircraft for that one (the flight to LAX already being two hours late, they figured they'd spread the misery out a bit, instead).

Our flight was scheduled to leave DTW at about 9 pm; we eventually left at around 11-11:30, arriving in Boston at about 1 in the morning.

The A320, originally scheduled to be the 7:30 flight from Detroit, was listed on the monitors at Boston's Logan airport to be arriving at 3 am (meaning it had not left the ground in DTW when we arrived in Boston).

The DC-10 had had its own problems, but they were (obviously) better understood by the ground crews involved.

An issue of RISKS management: on my last flight through Detroit, I saw a brand new ("two months old") 747-400 being loaded for a flight to Minneapolis (one of Northwest's other hub cities). After checking the schedule, it turns out that this plane is currently being used *only* to shuttle between the two cities.

Anyone want to bet it's for ground-crew and maintenance crew familiarization at two airports likely to see many more of the -400s?

--Chris

< Christopher Davis, BU SMG '90 <ckd@cs.bu.edu> <...!bu.edu!bu-cs!ckd> >

🗡 Ada MultiTasking

LAUGHLIN, CHET <ctl8588@rigel.tamu.edu> 14 Oct 90 21:51:23 GMT

In responce to Erling Kirstainsen's article about Ada's multitasking being vaguely defined - my Real-Time systems class has had problems with exactly this issue. In general the class is a graduate level course and we had hoped to use Ada on a network of IBM PS/2s for the labs.

The first lab involved two tasks running in parrellel. In reality it was figured that the tasks would time-slice on a single machine. However, this was not the case. The compiler would simply run the highest priority task until it ended, and then run the lower task. It was interesting to note that programs

that ran correctly on SUNS did not run correctly on the PS/2s - even though they compiled without change.

Now, one could blame the operating system - DOS is not anywhere close to a multitasking system. Or one could blame the language. The compiler makes no mention of the fact that tasks will not run concurrently in any of its documentation - and so I'd lean toward placing blame there. I suppose that if Unix or OS/2 could be afforded and placed on the PCs the programs would compile and work correctly. We have also discussed in class how the specification for Ada is open to interpretation on how tasks should be scheduled.

The end result is that the labs will be done in C on the PS/2s.

Chet Laughlin CTL8588@RIGEL.TAMU.EDU

Re: Expert system in the loop

Randall Davis <davis@ai.mit.edu> Mon, 8 Oct 90 13:21:46 edt

Two (last?) gasps:

1) As the previous discussion (two years ago) of this incident made clear, another fundamental problem here is the tactical advantage of offense over defense: the distance from which it's possible to shoot accurately is larger than the distance at which it's possible to identify the source. That may not have been a crucial factor in this incident, but it contributes to the mindset and practice that says self-defense means you may have to fire at a threat before you're certain of its identity. That's a consequence of all sorts of technology, and it happens to the infantryman with a rifle because bullets can fly further than we can easily see.

As for the title of this whole discussion -- "Expert systems in the loop":

2) There aren't any and there never were any. As abundant discussion has made clear (particularly the description by Matt Jaffe in 10.46), the Vincennes had some interesting signal processing and data description hardware and software, but nothing that can by any stretch deserve the term "expert system." If there's more software to the story than anyone has described thus far, it would be interesting to hear about it from a knowledgable source. We might also consider this, from an early report about the system (from a story in Risks 9.70):

"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."

Note in particular the second sentence, indicating that the system displays data about the aircraft, not threat interpretation. As noted in earlier discussions, this data (like the data on your speedometer) can of course be incorrect, but that's a different issue.

So until otherwise informed, let's be clear about this: it was a problem of "Instruments in the loop". That by itself may be worth discussing, but it is not and never was an expert system. And it might be interesting to ask, Why the rush to label it an expert system?

Announcement of CPSR annual meeting

<kalmin@atd.dec.com> Mon, 15 Oct 90 09:37:10 PDT

> 1990 Annual Meeting of Computer Professionals for Social Responsibility October 20 and 21 Stanford University and Palo Alto, CA

Computer Professionals for Social Responsibility, the nation's only public interest organization of computing professionals, will hold its 1990 Annual Meeting at Stanford University and at Ming's Villa restaurant in Palo Alto on October 20 and 21, 1990.

The CPSR Annual Meeting is a national meeting that gives computer professionals from all over the country a chance to meet and discuss some of the most important and interesting issues facing the profession and the public. This year's meeting will cover civil liberties and First Amendment rights in computer communication; using computers to support democratic oversight of government; women in the computing field; and what the public is at Stanford University, will include the following:

John Perry Barlow -- "Civilizing Cyberspace: Computers, Civil Liberties and Freedom." Barlow is the co-founder of the Electronic Frontier Foundation, a lyricist with the Grateful Dead, and author of the article "Crime and Puzzlement" featured in the latest issue of The Whole Earth Review.

David Burnham -- "Turning the Tables: Computer Oversight for Citizens." Burnham is a former investigative reporter for the New York Times, and the author of the books The Rise of the Computer State and A Law Unto Itself, the latter an expose of the IRS. While at the Times, Burnham was responsible for the stories that led to the Knapp Commission on police corruption in New York City, and he was the reporter who broke the Karen Silkwood story. He now works with the Transactional Records Clearinghouse at Syracuse University. TRAC uses the Freedom of Information Act and computer analysis to provide oversight of powerful Federal agencies such as the IRS, the Nuclear Regulatory Commission, and the Department of Justice.

There will be two panel discussions the afternoon of Saturday, October 20:

"Women in Computing: Where We Are, Where We Want To Be, and How To Get There."

Panelists:

Shari Lawrence Pfleeger, Chair, ACM Committee on the Status of Women and Minorities

Donna Lehnoff, Women's Legal Defense Fund

Sheila Humphreys, Department of Electrical Engineering and Computer Science, UC Berkeley

Barbara Simons, Secretary, Association for Computing Machinery (ACM)

Panel moderated by Anita Borg, DEC Western Research Lab

"The Media and 'Mythinformation': What and How Does the Public Learn About Computers?"

Panelists:

Bob Abel, multi-media expert and television commercial producer, Synapse Technologies

Michael Rogers, general editor and technology editor, Newsweek magazine

Rudy Rucker, physicist and science fiction author

Rob Swigert, professor of creative writing, San Jose State, science fiction author, and author of Portal, interactive fiction

Panel moderated by Paul Saffo, Institute for the Future

The Saturday program begins at 9 a.m., and a continental breakfast will be served just prior to the meeting. There will be a lunch break from noon to 2 p.m., and the meeting is scheduled to end at 5:30.

The Sunday, October 21, portion of the two-day meeting will be dedicated to discussions about CPSR as an organization, and there will be workshops on computers and education, the environment, civil liberties and privacy, peace and war, and computers in the workplace.

Admission to the CPSR Annual Meeting is \$35 for members, \$45 for non-members until October 14. After October 14 prices go up \$10 for each category. Non-members can join CPSR for one year for \$40 and pay the member price to

the meeting. Admission to the banquet is \$50 per person, the same price for members and non-members.

In addition, for \$100 more people can attend a fundraising reception for CPSR at the offices of Regis McKenna, Inc., on Saturday evening from 6 to 8 p.m. This is a chance to meet the speakers, leaders of CPSR, and many people from the computer industry of Silicon Valley. Contributions to CPSR are tax-deductible.

For more information and registration materials, contact CPSR at (415) 322-3778 or by electronic mail at cpsr-staff@csli.stanford.edu.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<anonymous> Tue, 16 Oct 1990 16:52:53 PDT

Computer blunders, revealing Kasparov's sealed move

Moscow, 16 october 1990 (tass)

The computer used for the world chess title match between Kasparov and Karpov accidentally disclosed a move sealed by the reigning champion in the adjourned third game, Izvestia reports from New York today. Izvestia writes in its evening issue that Kasparov "moves the king to attack the white rook". This means the sealed move was 41...kd6.

[Perhaps he was using the Gary Indiana Jones Beach Defense, and the computer had never seen seals there before. PGN]

X Software problem contributes to woman's death

Mike Overstreet <cmo@xanth.cs.odu.edu> Mon, 15 Oct 90 18:22:29 EDT

The following is taken without permission from the October 14, 1990, edition of The Virginian-Pilot and The Ledger-Star, Norfolk, VA.

"NORFOLK -- Glitches in the city's new emergency computer system and a dispatcher's mistake caused rescue workers to take 30 minutes to get to a 65-year-old heart attack victim in July, according to city records, and the delay may have been responsible for her death.

"Shortly after 9 p.m. on July 7, Dorothy G. Morris of 8256 Wedgewood Drive became short of breath and called to her son, Michael, for help. Michael Morris, who lived with his mother, dialed the 911 emergency telephone number three time before an ambulance was dispatched. ...

"... City documents show that after Dorothy Morris' death, city officials tried to pinpoint the cause of the delay. They interviewed dispatchers and checked call records and tapes of 911 phone calls. They also interviewed Michael Morris.

"Records indicate that they discovered an internal audit, or `logging,' program -- designed to track messages through the city's new computeraided dispatch system -- had not been installed as promised by the software vendor, PRC Public Management Services of McLean Va. The new \$760,000 system, called CADMAS, has been on-line since May 1.

"The omission was the latest problem encountered with the system and with PRC, said Martin Mendelsohn, director of the city's Department of General Services. He said the problems, which appeared after CADMAS was installed, included: too much computer down time; difficulties with a backup computer, which repeatedly failed to kick in automatically when the first computer crashed; turnovers and conflicts with PRC project managers; and the missing audit system.

"But the most disturbing problem was the tendency for some message to disappear after they were entered into CADMAS, city officials and dispatchers have said. Police have said that messages for detectives and forensic investigators often disappeared between dispatchers' shift changes, and that the disappearances are continuing. Mendelsohn of Friday said he was aware of fewer then five messages that disappeared between May 1 and July 12, when the audit system was installed.

"Mendelsohn said he was not aware of any disappearances after July 12.

"City officials said that, even after an investigation, they are not sure what happened to the 911 message typed by the dispatcher when Michael Morris first called.

"`The logging system would have tracked the message, but ... the logging system was not operational,' Mendelsohn said. `We could not prove whether the dispatcher entered the message improperly or whether it was somehow lost in the system.'

Airliner story (<u>RISKS-10.49</u>)

Christopher C. Stacy <cstacy@ai.mit.edu> Fri, 12 Oct 90 00:36:36 EDT

Gene Spafford writes about his decision to never again fly on Northwest airlines, citing that they have just purchased "a bunch of" A320s for domestic use. (The A320 is a controversial fly-by-wire airplane.)

He forwarded us a "horror story" from his friend Rich Epstein, who appears to have been badly frightened by an airline experience in which rain leaked into the airplane and disabled the transponder and auto-pilot computer. In the story, the airliner departed from Chicago O'Hare enroute to Washington Dulles, but then has to turn back to O'Hare 15 minutes later because the air traffic controllers have lost radar contact with the flight. On the way back, the pilot made an announcement about the airplane having steel control cables, which Rich interprets as "a reference to the fact that an Airbus would probably have been disabled completely in a similar circumstance." In conclusion, Rich describes the further trauma of exiting the airplane at the terminal, having to pass through a thick sheet of rain, some of which was leaking into the airplane, which he speculates may not have been docked correctly.

I am very skeptical about the safety of new airplane systems such as fly-by-wire, and I also wonder about the quality of the maintenence and procedures of the airlines, especially in light of the recent serious fines against Eastern.

However, I am not sure that Gene's message or his friend's story sheds any light on these issues or supports any conclusions about the A320. The message did not make clear to me exactly what risks Gene finds unacceptable. The tone of fear and alarm, coupled with a lack of information about air traffic procedures, may lead to misunderstandings. I don't have any more information about what happened on that flight than what I read in the story. However, my interpretation would be a little bit different.

The radar scopes that the air traffic controllers at O'Hare are watching, display targets based on both primary returns (the signal bouncing off the airplane), and secondary returns from the onboard transponder. The transponder makes detection more reliable, and also transmits such data as the flight identification number and present altitude.

Radar contact is not a necesary to conduct a flight, even in bad weather. Radar is not used for navigation, nor is it required for landing. It does increase safety, and allows greater utilization of the airspace, since the controllers can track the progress of a plane more directly. Before the airliner took off, the details of its flight plan were arranged and airspace was reserved for it. The flight could have been conducted safely without radar, even if radio communications had been lost.

The auto-pilot computer is not a critical part of the airplane, and it's loss is not very interesting. It merely means the pilots would

have to actually put their hands on the controls and fly the plane.

The flight was returned to the departure point in order to avoid any additional problems. The pilot probably declared an emergency for priority handling because nobody fully understood the extent of the failures. This accounts for the emergency vehicles at the airport.

Most people have various degrees of fear regarding flying, and knowing that something has gone wrong with the plane, not understanding any of the details, being disconcerted about hanging around in the clouds, seeing the flashing lights of emergency vehicles, not having any control over your fate, and finally getting rained on when you disembark your canceled flight, can all combine to thoroughly upset even a seasoned air traveler.

My alternate interpretation of the pilot's remark about the "stainless steel" cables, is that he was attempting to calm the passengers by making a joke about the airplane controls not rusting in the rain.

Maybe Gene is trying to make the analogy that if a computer in a regular airplane can get rained on and fail, that this would be catastrophic in a computer-controlled plane like the A320. However, this story does not support that idea, and it presents nothing particularly relavent to the safety of the A320, the airplane in the story, or the airline. Except perhaps to note that an onboard systems failure was easily handled, and resulted in nothing but inconvenienced passengers. Any proposed analogy to systems failures on the A320 is far too general to be very useful, since the A320 and the airplane in the story don't have the same design or the same kind of computer systems.

Re: Airliner Story (<u>RISKS-10.49</u>)

Richard Neitzel <thor@thor.atd.ucar.edu> 16 Oct 90 14:15:04 GMT

I find the dissemination of this kind of misinformation troubling, especially when it apparently comes from a source that should know the correct information. The aircraft in question was most certainly not "invisible". How "an Air Force ROTC student" could claim radar requires transponders is beyond comprehension (so that's how stealth technology works - turn off the transponder!). However, what is most disturbing about this is not the apparent ignorance of a (hopefully) poor student, but the easy accept ence of this "expert" information by non-experts. Since the original source of this story allowed one of his friends to forward it to RISKS, it is very likely that many other channels of communication has been used to speard this story. Undoubtabley there are now more people who are now even less confident in the air traffic control system, based on completely erroneous information. It seems to me that this is a much greater risk then it might appear on simple reflection. As our society becomes increasingly technical, it becomes less possible for each individual to determine if information outside their area of expertise is correct. Unfortunately, I submit that most "technical" information that is disseminated is in fact either incorrect or, even worse, deliberately distorted. Try watching reading your local newspaper or watching TV news

programs and pay close attention to the level of accuracy in technical matters. A very good example to the current "debate" on the greenhouse effect - people with a political agenda are attempting to lead the public's opinion by selective use of information. Indeed, some "greenhouse backers" have been candid enough to admit that they do not feel that real evidence of any such phenomena is required, rather a public perception of a problem is all they require. Remember the ridicule when then President Reagen said that plants were the largest contributors of carbon dioxide "polluiton". Well, there is growing evidence that the rise in CO2 may well be largely due to purely natural effects caused by plants - a process that man likely cannot alter for good or ill. But this is not politcally correct science, so it is buried in silence. And witness the neat trick used in another recent RISKS article about bank computer security - banks have security problems, they don't want them discussed, so if they deny there are any this is proof they don't like to discuss problems (you are mentally ill and the fact that you deny this is proof that you are mentally ill). It is very likely that most readers of this piece simply believed the implication that such massive breaches of systems is common and (for the hacker) simple. Unfortunately, there is no proof of the claims. Many of these stories have a suspicously similar format and are strikingly like many of the popular urban myths - no hard evidence, but "I heard from someone that they heard".

Faced with the pronouncements of experts or those percieved as experts, how can outsiders make correct decisions, if the experts are supplying false or misleading information? Perhaps we should all start examining our sources more critically, but more important, we should make certain that we are not responseable for spreading misinformation. Are you certain that the person to whom you just explained a techincal matter outside their field really understood what you said? Do you pass on as "true", information you only partially (mis)understand. Above I implied that the ROTC student was to blame for the mistaken information about radar, but perhaps the listener gleaned that "fact" when something quite different was said. The wise man speaks only what he knows is the truth and knows his own ignorance.

Richard Neitzel National Center For Atmospheric Research Box 3000 Boulder, CO 80307-3000 303-497-2057

Re: A320s and Northwest Airlines (<u>RISKS-10.50</u>)

"Craig A. Finseth" <fin@unet.unet.umn.edu> Tue, 16 Oct 90 09:16:51 -0500

I hate to deflate a good story, but there is another reason why 747-400s are used on the Minneapolis to Detroit run. The 747-400s are mainly intended for trans-Pacific use. However, each aircraft that is intended for such international use must first be operated within the US before it is certified by the FAA. I believe that the operation is both in total hours and in takeoffs/landings. Hence, using short runs allows the airplane to accumulate many takeoffs and landings. In addition, the large capacity of the aircraft allows better use of the heavily-travelled corridor (I believe that they take two smaller planes off the run). Craig A. Finseth, University Networking Services, University of Minnesota 130 Lind Hall, 207 Church St SE Minneapolis MN 55455-0134 +1 612 624 3375

✓ Technophilia-induced problem at Educom?

<r.aminzade@lynx.northeastern.edu> Tue, 16 Oct 90 13:55:32 EDT

Today's EDUCOM keynote speech, by former President Jimmy Carter was open-captioned for the hearing impaired. The big-video display in the auditorium showed a textual representation of the speech as Carter spoke. This was provided by "11-Alive," an Atlanta television station.

The system must have used some kind of voice-recognition algorithm, because no human typist that I know could have kept up with the speaker at times. The weakness of the voice-recognition system was made painfully obvious to attendees, when those with the ability to hear the presentation noticed substitutions like:

"man well" noriega, "wak dem iks" for academics, "oath yope yam" for Ethiopia, "Jap neens" for Japanese, "My Robe by" N Nairobi for "Ken Yeah" for Kenya, "Home Jean yes" for homogeneous.

Carter's speech was thoughtful and moving (he talked about academia's moral responsibilities to the third world), but the seriousness of the speech was undercut by the occasional giggle from the audience.

Later in the speech, human control seemed to be asserted a bit more, and "another country" was frequently substituted for the name of a third-world country, but Carter must have been most puzzled when he explained that the Carter Foundation was nonpartisan, and that "Prominent Republicans" worked closely with him on every major project. It was presented to the hearing-impaired (and to the rest of us) as "Prominent Rubble Cans." Of course, the audience broke into laughter, and I suspect he still doesn't know why.

I'm a strong supporter for appropriate adaptive technology, but a low-tech solution (an ASL interpreter) would have been less distracting and reached many (though not all) of the hearing-impaired.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



SPELT P F <sfp@stc06.CTD.ORNL.GOV> Wed, 17 Oct 90 09:50:46 EDT

In his article posted in RISKS forum of 15th October 1990, Robert Dorsett made a comment about the A320/human interface which triggered a "respond NOW" action in me. I am a psychologist working at ORNL in human factors -- the study of the way people and their machinery (for work or play) interact. Dorsett said:

>I suggest (again) that the way the airplane interacts with the pilot is >at LEAST as important as component-wise reliability.

I say: YOU BET!!! My work in human factors (HF) for various projects, some involving computerized interfaces, some not, has yielded various comments. The worst kind is: "HF is just common snese." Oh, yea? Then why have we had SO MANY instances of poorly designed devices creating "human error", aka "pilot error" in the cases of the A320 and other aircraft crashes? Another major porblem, also suggested in Dorsett's posting, is the use of HF consultation. The prevailing modus operandi has traditionally been to design the system, call in the HF

consultants for evaluation, then have them design a training program to "train around" the problems designed into the system. Such training will "work" adequately until a major off-normal event (like TMI), when the operator is unable to react properly to (interact properly with?) the mis-designed system.

As we come to design and install more and more complex computerized interfaces between the machinery and the humans using it, we run the serious risk of making even greater design errors, many of which will not show up at all until a major off-normal occurrence comes along. The introduction of artificial intelligence (AI) into these interfaces adds an additional dimension along which design errors will propagate. These concerns have been very adequately covered in the postings on the Aegis system (Expert System in the Loop postings), although there WAS no ES in that system.

Several of us at ORNL are involved in research into the use of AI in "operator associates" for various settings. The potential for using intelligent icomputerized interfaces is already being explored in a variety of settings, but many issues remain to be settled, as the Aegis discussion has highlighted. These issues need BASIC research directed to answer the questions raised. In this era of increasingly tight budgets, however, finding support for that basic research is very difficult. Hrowever, if we don't address these issues, there will continue to be an increased number of "operator error" accidents analogous to the A320 "pilot error" crashes.

The usual disclaimers apply: These opinions are my own, and do not necessarily reflect those of ORNL, the Department of Energy, or Martin Marietta Energy Systems.

email: sfp@stc10.ctd.ornl.gov@UMCGATE@OAX Phil Spelt bldg 6025, ms 6364 POBox 2008 Oak Ridge, TN 37831-6364

Me careful of what you give away!

&.FREEMAN@csi.compuserve.com> 17 Oct 90 10:33:07 EDT

>From CompuServe's Online Today Forum Data Libraries:

MONITOR MONTH IN REVIEW September 1990

FEDS SEIZE COMPUTERS IN KY. TOWN (Sept. 2): Federal agents over the weekend seized computer equipment from a Nancy, Ky., business office when it was learned that the computers might contain secret government files. The owner of Challenger Ltd., Charles Hayes, said federal marshals came 70 miles from the US attorney's office in Lexington, Ky., to seize nine computer terminals, a computer memory device and other equipment which were purchased from the government for \$45."

This shows a Risk from computer equipment you are trying to get rid of. Make sure you are only getting rid of the equipment, and not giving away copies of your data! A tape bulk-eraser probably does a nice job on old tapes and hard drives.

Mark FreemanMicrocomupter Technology Specialist/AnalystCompuServeM.Freeman@CSI.CompuServe.COM

Ke: Technophilia-induced problem at Educom?

Benjamin Ellsworth <ben@hpcvlx.cv.hp.com> Wed, 17 Oct 90 10:02:19 pdt

> The system must have used some kind of voice-recognition algorithm,
 > because no human typist that I know could have kept up with the
 > speaker at times.

I very strongly doubt this. I would bet a substantial sum of money that there was a stenographer and not a computer capturing the words.

> The weakness of the voice-recognition system was made painfully> obvious...

There is RISK of assuming all failures are technologically induced. It could very well be that the stenographer hired was simply not very good. The good ones are expensive, and to do "real-time" stenography takes a good stenographer.

There is a plausible explanation involving computer RISKs however. The translation from the steno notation to full english words was in all likelyhood automated. In stenography there are a number of dialects (usually called theories). Some dialects, especially the older ones, are not particularly suitable to machine translation. There are also more than a few translation programs. Between stenographic dialects and computer translators there can be a significant compatibility problem. It could be that the stenographer was extremely capable in the courtroom (where the translations are done off-line by a human), while at the same time using a style/dialect/theory which was incompatible with the machine translator.

There has been an interesting interaction between technology and court recording in the last couple of decades. My mother, for instance, is in the process of re-learning her stenography in a computer compatible dialect. It reminds me of pilots who have to learn to fly in a computer compatible way (training around system weaknesses).

Benjamin Ellsworth ben@cv.hp.com All relevant disclaimers apply.

Passwords and chess

<smb@ulysses.att.com> Tue, 16 Oct 90 22:46:39 EDT

Well, since we're talking about chess, here's a tidbit from Saturday's NY Times, in an article about the Kasparov-Karpov match:

Trying to meet a noon deadline yesterday for invoking the time-out, Lajos Portisch, a Hungarian grandmaster who is Mr. Karpov's second, telephoned Geurt Gijssen, a Dutchman who is chief arbiter of the match, at 11:53 A.M.

How was the arbiter to be sure it really was Mr. Portisch on the line?

The Hungarian, who had considered a singing career early in life -- a fact known to some chess experts -- suggested singing something in his distinctive voice. Mr. Gijssen agreed, and Mr. Portisch burst forth with several bars of a Hungarian song.

The arbiter granted the postponement, although the written request for the time-out arrived late, at 12:07 P.M.

Sounds like they need some sort of challenge/response scheme; that password is blown...

--Steve Bellovin

"Expert Systems in the Loop" explained

Martyn Thomas <mct@praxis.co.uk> Wed, 17 Oct 90 18:28:08 +0100

davis@ai.mit.edu (Randall Davis) writes:

>As for the title of this whole discussion -- "Expert systems in the loop":

>2) There aren't any and there never were any.

>

>So until otherwise informed, let's be clear about this: it was a problem of >"Instruments in the loop". That by itself may be worth discussing, but it is >not and never was an expert system. And it might be interesting to ask, Why >the rush to label it an expert system?

The original article was mine, and referred to a report of a new research project in the UK to develop an expert system to advise commanders in tactical situations which are too complex to analyse without assistance.

This report *explicitly* referred to an expert system. The point of my original posting was that an expert system which provides advice, in

circumstances where a decision must be made and there is insufficient time for the commander to analyse the situation him/herself, is effectively making the decision. Many who followed up agreed with this viewpoint. I apologise for mentioning the USS Vincennes - it distracted attention from the major point, and wasted a lot of net bandwidth. So far as I recall, noone, throughout the discussion, suggested that Aegis is an expert system.



Search RISKS using swish-e

Report problems with the web pages to the maintainer


Robert Dorsett <rdd@ccwf.cc.utexas.edu> Wed, 17 Oct 90 16:50:58 -0500

>From FLIGHT INTERNATIONAL, September 26, 1990

CALL FOR COMPUTER CABIN-SAFETY TEST

"Future cabin safety testing for new airliners should be determined by computer-based analysis, according to Michel Le Clerc, Airbus Industrie's deputy chief engineer, widebodies.

"Practical evacuation tests are limited in their scope, produce unreliable conclusions, are dangerous for participants and extremely expensive, said Le Clerc at the conference.

"Le Clerc wants intensive studies of evacuation tests and actual accidents to be conducted, saying, 'Steps should be taken to set up a database and computer model available to everyone. Sufficient data already exsits for the necessary analysis' ...although unconventional configurations may require testing," he adds. "A full certification test evacuation program costs about \$1 million for a narrowbody and \$2 million for a widebody, points out Le Clerc, and about one in ten people are injured."

Just a couple of comments. :-)

1. \$1-\$2 million is about 0.03% to 0.1% of the total development costs for a new aircraft. On a 2000-aircraft production run, the per-aircraft cost will be about a thousand dollars, or .0014% of the cost of a \$70 million airplane. We're talking peanuts, here.

2. The notion that a *computerized* model will work, whereas earlier models have failed, is of concern. Statistical analysis of exits is nothing new. However, time and time again, such analyses tend to cut corners, to rely on ideal conditions, and use admittedly imperfect evidence (the same "data", I'm afraid, that Le Clerc's referring to). Problems are usually shown in practical demonstrations. However, by using "data" and putting it into a "computer," it becomes much more difficult to refute that model's "conclusions."

3. Part of the reason for Airbus's desire to rely on models is its enormous investment in a massive CAD/CAM/documentation system.

4. The last major fiasco which involved the use of raw statistics to set evacuation policies was when Northwest, and other operators, petitioned the FAA to seal the over-wing exit doors of 747-200's. The FAA's northwest district approved it, but the national branch overturned the approval, citing unnecessary risk.

The entire industry has also been collaborating in certifying twin-engine airplanes for extended-range over-water operations, a controversial issue at best. This summer, a proposal arose to also use models in lieu of practical demonstrations.

I think it's only a matter of time before a major manufacturer petitions for a waiver of major airframe "practical" tests in favor of simulations. After all, if they can build it, the theory can't be wrong, right? Or something like that.

Re: Ada and Multitasking

Edward V. Berard <eberard@bse.com> Fri, 12 Oct 90 05:44:44 EDT

> The author then describes several features of the Ada language, such as data

> typing, separate compilation units, and concurrent tasks.

> The RISKy bit comes in the discussion of task priorities. [...]

This "problem" is more one of a misunderstanding of the capabilities of the Ada language than an actual language definition problem. A serious user of Ada

should know that some things, especially in the area of tasking, are defined in a non-deterministic manner. This is usually phrased in terms like "if several select alternatives are open, one will be selected in a non-deterministic manner."

Yes, each implementer (of an Ada compiler) does indeed have a certain amount of freedom in choosing how to do scheduling, and the Ada programmer has the option of leaving it entirely up to the compiler to select a particular alternative. Further, this definitely has the potential of different behaviors as a result of using the same source code with different Ada compilers.

However, if this is truly unacceptable to the program's author, it is entirely possible to write the same code in such a way that it behaves in exactly the same manner on all Ada systems. This does not even require "tricky code."

Writing portable and predictable code using Ada is definitely possible, and, and for that matter, is done all the time. Please be aware of the fact that Ada does not force you to write only deterministic tasking code, but does provide you the capability to do so if you desire.

> ... A language which boasts high portability and reliability includes
> features which mean that there is no guarantee that a program will work the
> same way if ported to another compiler and/or run-time environment.

If I went out of my way not to learn the proper semantics of the language, and worked at writing non-portable code, this would be true.

The crux of the matter is really flexibility. If the designer of the Ada language (Jean Ichbiah) decided that there was only one way to set priorities, he could have built that into the language. Unfortunately, not everyone would have agreed on that mechanism. So, Ada was designed in a manner which gives the programmer a choice:

- a. Allow the underlying implementation to select among a set of choices in a non-deterministic manner, or
- b. Force a particular, programmer-defined set of priorities, which can always be the same regardless of the compiler implementation

> Does anybody have any experience (good or bad) in porting Ada programs, in > particular real-time programs?

My experience (hundreds of thousand of lines of code ported to many different platforms) shows that it is possible to routinely write very portable, predictable Ada code. However, I have seen the following:

- * A poorly trained Ada programmer determines the underlying scheduling algorithm for his or her Ada compiler and writes code to take advantage of this scheduling algorithm. Problems occurred when:
 - a new version of the compiler came out with a different scheduling algorithm,
 - the source code was ported to an Ada compiler with a different

scheduling algorithm, and/or

- the programmer did not understand (or correctly identify) the underlying scheduling algorithm.

* An Ada programmer realized that Ada compiler writers have a certain amount of flexibility when it comes to some (not all) priority issues, and then wrote very deterministic code. However, the actual application called for non-deterministic code. (This problem is very similar to having a "not-so-random" random number generator.)

There are definitely risks associated with this issue. However, one must be careful in identifying the source. For example, if an Ada programmer is poorly trained, should we blame the language, the programmer, or management? -- Ed

Edward V. Berard, Berard Software Engineering, Inc. 18620 Mateney Road Germantown, Maryland 20874 Phone: (301) 353-9652

×

Fri, 12 Oct 90 15:30:27 PDT

Inc.) Subject: Re: Ada and multitasking (<u>RISKS 10.48</u>)

In his contribution to <u>RISKS 10.48</u>, Erling Kristiansen criticizes Ada's concurrency features (the tasking mechanism) as hampering reliability because the language definition leaves room for more than one possible program response to the same sequence of events, depending for example on the way the scheduler handles task priorities to reflect various possible fairness policies. In his words, this highlights a contradiction between portability and reliability.

Regardless of one's opinion about Ada's support for reliable programming (concurrent or not), which certainly leaves room for criticism, Mr. Kristiansen's comments seem based on an over-restricted view of reliability. In his opinion,

"A language which boasts high portability and reliability [must not] include features which mean that there is no guarantee that a program will work the same way if ported to another compiler and/or run-time environment."

Depending on how one defines ``work the same way'', this requirement is either appropriate or too strong.

It is too strong if ``working the same way'' means always executing the same actions in the same order as a response to the same input events. After all, isn't non-determinism a fundamental aspect of concurrency? Even in a purely sequential world, one can hardly guarantee that computations (on floating-point numbers, for example) will execute identically on all computers.

The only productive way of transforming the above into a realistic

requirement is to accept that a program, or program element, is based on a higher-level description of intended semantics - in other words, a specification. (I have called this ``programming by contract'' in various publications, some of which, incidentally, directly criticize another aspect of Ada, its exception mechanism, precisely for its possible risks to reliability.) A specification states the required properties of the acceptable observable behaviors of a software system. It does not need to prescribe only one behavior as acceptable.

Different implementations that behave differently, and possibly even produce different observable results, are then acceptable as long as they conform to the specification.

Two of the possible reasons to leave certain properties open in the specification are portability and the need to support various scheduling or fairness policies. They do not conflict with the reliability requirement. To take an obvious non-computer analogy, you may tell a taxi driver to get you to point X in at most half an hour, without specifiying the itinerary, which is not part of your definition of ``reliability'' for this trip.

All this assumes, of course, that there is a way to express precise specifications, which Ada does not provide, although some Ada-based tools, notably Anna, do.

-- Bertrand Meyer

bertrand@eiffel.com

🗡 Ada MultiTasking

<firth@SEI.CMU.EDU> Tue, 16 Oct 90 08:07:29 -0400

> ... Or one could blame the language.

Or, of course, one could ask that the instructor take the trouble to learn the language he proposes to teach! The Ada Reference Manual [RM 9.8(4)] mandates exactly this behaviour:

If two tasks with different priorities are both eligible for execution and could sensibly be executed using the same physical processors and the same other processing resources, then it cannot be the case that the task with the lower priority is executing while the task with the higher priority is not.

In other words, and without any vagueness whatever - run the higher priority task until it ends, and then run the lower priority task.

Robert Firth

🗡 Re: Ada MultiTasking

Ray Diederich <diederich_r_%ncsd.dnet@gte.com> Tue, 16 Oct 90 14:54:42 -0400

In <u>RISKS 10.50</u>, Chet Laughlin <ctl8588@rigel.tamu.edu> writes: >The first lab involved two tasks running in pa[r]ellel. In reality it was >figured that the tasks would time-slice on a single machine. However, this >was not the case. The compiler would simply run the highest priority task >until it ended, and then run the lower task. ...

In response, ANSI/MIL-STD-1815A, chapter 9, paragraph 2 states: >Tasks are entities whose executions proceed *in parallel* in the following >sense. Each task can be considered to be executed by a logical processor of >its own. Different tasks (different logical processors) proceed >independently, except at points where they synchronize.

Nowhere in this paragraph nor the surrounding text is the idea of time-slicing mentioned nor implied. Depending on time-slicing is erroneous programming, because it means depending on characteristics which are out of the control of the programmer. Further, resorting to time slicing is simply a way of saying "I don't know how to best schedule these tasks; you, the compiler, may schedule them for me." Ada supplies several synchronizing tools which allow logically concurrent processing without depending on time-slicing.

Time-slicing gives you a means of relieving your responsibility to solve your real-time processing design problems -- at the expense of added overhead, less control of your program, and less reliability in your system. Yet, every time I come up against a problem which requires real-time performance, I find that most of my peers start chanting "we need to time-slice, we need to time-slice."

I challenge any circumstance which would require time-slicing to be "correct." If the point of Mr. Laughlin's project was intended to teach the real-time use of the multiprocessor environment (by simulating multiprocessing with tasks), I suggest that his choice of problems is flawed. A good real-time multiprocessor problem requires interprocess dependency (which may be implemented by Ada task rendezvous). Without the interprocess dependency, you might as well cut the cables and run with stand-alone processors.

In response to Erling Kirstainsen's article which originated the topic, any time one resorts to erroneous programming methods, one sacrifices reliability and portability. It's not the fault of the language nor the associated hype.

Ke: Ada MultiTasking (Laughlin, <u>RISKS-10.50</u>)

Brian Hanafee <bhanafee@ads.com> Tue, 16 Oct 90 12:19:25 -0700

The basic error is contained in the statement: "In reality it was figured that the tasks would time-slice on a single machine." This assumption is in direct contradiction of the Ada LRM, section 9.8, paragraph 4:

"If two tasks with different priorities are both eligible for execution and could sensibly be executed using the same physical processors and the same other processing resources, then it cannot be the case that the task with the lower priority is executing while the task with the higher priority is not."

Running the higher priority task until it ended was the correct behavior!

Much of the difficulty people have with Ada tasking is (in my opinion) related to the fact that the Ada tasking model does not assume (nor preclude) a time-slicing mechanism. I believe the Apple Macintosh Multifinder implementation is another example of multitasking without time slicing.

The decision to use or not use time slicing should be based on a number of factors including the availability of a clock to cause interrupts, the cost of saving the machine state, and the benefit of "fair" scheduling. The availability of an appropriate clock is not a given for all computer systems, particularly embedded systems. Furthermore, the cost of saving the machine state at a random point in the execution of the program is almost always greater than the cost of saving state only at predefined points such as task entry and exits. The benefit of "fair" scheduling occurs frequently in multi-user systems where users are often competing for the same resources, however in dedicated or embedded systems, the designers could use tasking and programming discipline to enforce "fair" scheduling without requiring the additional overhead of time-slicing. The decision to use or not use time slicing is usually made by the compiler vendor (although ideally it should be switchable by the compiler user); programs in Ada (or any other language) which depend on a particular implementation are erroneous.

Brian Hanafee

bhanafee@ads.com

Ke: Technophilia-induced problem at Educom? (RISKS-10.51)

"Miles R. Fidelman" <mfidelma@BBN.COM> 17 Oct 90 17:14:32 GMT

I've seen a talk where real-time transcription was provided by court stenographers. They used a version of a stenotype machine coupled to display software.

Stenotype machines have phonetic keyboards, and their raw output looks very much like what is described here. In courtroom practice, a clean transcript is made later. In the talk I saw, some software provided partial on-the-fly cleanup, but no where near perfect.

Another reader comments that an ASL translator would be preferable. My own take is that for technical talks this real-time transcription seems better able to catch technical vocabulary.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<forags@violet.Berkeley.Edu> Thu, 18 Oct 90 10:41:23 PDT

Al Stangenberger, Dept. of Forestry & Resource Mgt., Univ. of Calif. Berkeley, CA 94720 uucp: ucbvax!ucbviolet!forags BITNET: FORAGS AT UCBVIOLE

From KRTN News Wire, reported in Marin Independent-Journal (San Rafael, CA) 3 Oct 90 page B4:

SUNNYVALE - A strangely flawed computer chip was sold by the millions by National Semiconductor Corp. here between 1987 and last spring, with a potential for causing bizarre failures in computer systems. The chip's potential for mischief is significant because it was used by major computer makers for more than two years, and some may not be aware of the potential for problems. National first learned the chip had a design flaw in 1987, but it wasn't until January that the company stopped shipping it, according to a lawsuit filed in June by a former employee. The firm had a "large inventory" of the chips it didn't want to "dispose of as non-functional," claims the suit by Michael Parsin of Sunnyvale, a former managing engineer in the department product group responsible for the chip. "We did identify some isolated problems with that part among some customers," said Mary Coady, spokeswoman for National Semiconductor. "The company took steps to address the problem -- a bunch of steps. Of hundreds of customers for millions of parts that were shipped, I am told we have relatively few ... complaints", Coady said.

The chip tracks the time and date in computers and other electronic systems. In certain applications, it has had a tendency to skip forward one day, with unexpected results:

> The United Nations International Atomic Energy Agency used the chip in a new television security system for guarding nuclear fuel in atomic power plants worldwide, according to agency official Klaus Gaertner. Problems cropped up in one monitoring system, and design changes had to be made to protect the chip from electronic noise, Gaertner said. The chip is the suspected cause of the problem, but more testing may be needed to know for sure, said another engineer familiar with the system, who added that it would be very costly to replace them at this point.

> A Canadian company had difficulties with the chip on a military system. "It was a real problem," according to George Bleier, a project engineer with Marconi Canada who said it had problems in a system for a foreign military customer. "We were just flabbergasted." He said he complained by letter in 1988 and National fixed the problem, but only this year did the firm finally apologize.

> A financial program for a company was set up to print paychecks on
Fridays, but the chip caused the computer -- made by a major manufacturer to skip from Thursday to Saturday, leaving employees with no paychecks, according to an engineer familiar with the computer.

> A computerized trip recorder for long-distance trucks printed reports that made the truck look as though it were traveling at impossible speeds and "doing impossible things." The system frequently shut down, said an engineer at Rockwell International Corp. who worked on the system. The chip had to be replaced with another version. "It was a fiasco," said the engineer, who asked not to be identified. "If I go in there and say 'National time chip,' (my boss) goes through the roof."

National said "some isolated problems" have been reported in the chip -problems that seem to occur more frequently in even-numbered years. Exposure to electronic "noise" triggers a tendency to flip from 24- to 12hour time with unfortunate results, said some engineers who have used it. A new version does not have the problem.

M The slippery slope of personal identification and tracking

Jerry Leichter <leichter@lrw.com> Thu, 18 Oct 90 08:51:51 EDT

It was reported in last Sunday's New York Times that Princeton University has installed a new security system at one of its colleges (groups of related dorms and such). The doors to the college, heretofore always open, are now locked. Residents of the college have "proximity" access cards which unlock the doors. Such cards can be sensed from a reasonable distance (e.g., if you carry your card in your wallet, the door will unlock as you approach it). Others at the university can use their magnetically-encoded cards in a "swipe" reader to unlock the doors. Non-university people are supposed to be greeted at the entrance.

Princeton intends to install the same system at all its colleges over a period of time. The system is described by the university as "monitored 24 hours a day from a central location" (not an exact quote); precisely what this means and why anyone should care isn't clear, but apparently the university considers this a good thing which should instill confidence in the system.

The Times reports that some students at the college are complaining about the inconvenience caused by the system. The university justifies the system as necessary for safety - there have been several "incidents" on campus of late - and the inconvenience minor.

What no one mentions, at least in the article, is the potential such a system has for invading privacy. A card reader of this sort has the ability to track who goes where and when on a campus. Systems of this sort that I've seen log every use of a card. That log is subject to misuse. Suppose some government agency decides that student X is a dangerous radical, fomenting revolution. What a simple matter to track him and look for people who go to the same places he does - just check the logs. There's a long history of exactly this kind of investigatory technique - taking photographs of cars parked near demonstrations and checking for license plates that show up more than once, for example. It's also clear that, historically, most institutions have not resisted government attempts to gain access to such information; and that even when they do, the government can usually get a subpeona. Note that failing to collect information that a system can easily collect doesn't help - the government could easily demand that a logging system be turned on, just as it can require the telephone company, under appropriate court order, to track usage of a phone.

The fact that proximity cards are used makes the system all the more dangerous. First of all, you can be tracked without taking any specific action which means you'll have a hard time knowing when you might be tracked, and won't be able to avoid it. (Leaving the card home may not be a solution usually, it's an id card that you MUST have to accomplish almost anything). Second, it makes the system virtually invisible, so people don't think about the implications as much.

Now, I don't want to over-emphasize the dangers, such as they are, of the particular system at Princeton. The data will likely be fairly "course" - the cards give you access to a college, which is home to hundreds of people, not to individual rooms - and it PROBABLY won't be abused. But there's an

underlying issue here which has received too little discussion: One sideeffect of many recent technologies has been to make tracking of individuals a quick and painless matter. Every time you use your bank card, you are providing a central system with a real-time trace of where you are. These days, every time you use a credit card, it's checked with a central system again providing a trace. How many people know that their cellular telephones can be made to report, with no indication that they've been polled? This ability is an inherent part of the implementation of cellular systems, and even at its most limited allows the phone to be located to the nearest cell. In practice, with some effort one can usually locate the phone much more precisely, since some directional information is available and there is also usually signal strength information for several cells. The only way to keep the phone from responding is to turn it off.

Some losses of privacy are obvious; others are insidious, occurring as unintended side-effects of otherwise benign and even very useful technologies. The cumulative results can be the same, however.

In one of his science fiction books, Fred Hoyle speculates on how a universal "person tracking" system might come to be imposed. Initially, the system is created as a means to keep a small elite continuously accessible and safe. High government officials today accept a constant surrounding of protective forces and communication agents; making the tracking more automatic would only improve their situation. In Hoyle's argument, over time, more and more people are considered to be important enough to warrant the privilege of being part of the system; it's considered an honor. Eventually, though, EVERYONE becomes part of the system.

Constant accessibility, first with pagers, now with cellular phones, has indeed developed more or less along these lines. Constant position location, at least ACKNOWLEDGED constant position location, has not so far. Instead, it's creeping in even more insidiously, piggy-backing along with apparently unrelated systems.

-- Jerry

Technology Meets Dog; Dog Wins

Sanford Sherizen <0003965782@mcimail.com> Thu, 18 Oct 90 08:35 EST

Amid all of the problems posted here, a dog-bites-phone risk is worth noting.

NETWORK WORLD, October 15, 1990 had an article on AT&T Tariff 12 deals. In the article, the following appeared.

"On a lighter note, it seems a new type of long-distance fraud is making the rounds, as Tom and Bonnie Robb of Aliso Viejo, Calif., can attest.

When their telephone bill arrived recently, they had a difficult time figuring out who had made \$28 worth of toll calls to Sports Pick and the Adult Date line, according to a recent story in the HARTFORD COURANT.

But it turned out to be their cocker spaniel, who was using a large-faced push-button telephone. The Robbs had attempted to teach the dog to dial 911 by smearing peanut butter on the corresponding buttons of the keypad.

The dog had apparently taken to knocking the handset off the receiver and dialing telephone numbers, inadvertently dialing the 900 numbers."

W-H-Y were the Robb's attempting to teach their dog that trick? Are peanut butter manufacturers accessories to a crime? Did the dog enjoy the Adult Date Line? Are we sure that the dog *inadvertently* dialed those numbers? What animal species will next turn to crime?

Sandy

[Next the dog will learn how to imitate the touch tones, and its bark would be much worse than a byte. PGN]

Pilot error and human factors

<ark@research.att.com> Thu, 18 Oct 90 08:56:04 EDT

A few days ago I saw a comment on rec.aviation about `pilot error' from a flight instructor who had just come back from an AOPA recertification clinic. Among the notes from that clinic were that 75% of the pilots involved in accidents where the cause had been established as `pilot error' were at the time going through a marriage, divorce, or career change.

Airliner story (<u>RISKS-10.49</u>)

Bob Sutterfield <bob@morningstar.com> Thu, 18 Oct 90 14:24:14 GMT

Gene Spafford quotes RIch EPstein <@VM.CC.PURDUE.EDU:REPSTEIN@GWUVM>: Heavy rains leaked into the plane and knocked out the transponders and the auto-pilot computer. About 15 minutes into the flight the pilot announced that we had to return to O'Hare because the air traffic controllers couldn't "pick us up". In other words, we were invisible, in the clouds, at O'Hare... the pilot meant this literally. Radar picks up aircraft by means of the signal sent out by the transponders.

Lack of a transponder return isn't really an immediate, major safety problem. You weren't about to get bumped into. Your flight was operating under instrument flight rules (IFR), which means there was a very detailed flight plan and clearance in effect. Even if all two-way communications had been rendered inoperative along with the transponder at the moment of takeoff, a block of airspace would have been reserved for you as you moved along your route. Lost-comm procedures are a fundamental part of IFR flying, and provide a nearly algorithmic "way out" of every situation. Lacking a transponder but maintaining communications, the crew would simply have been required to provide regular verbal position reports, just like in the olden days (not so very long ago) when ATC radar coverage wasn't so pervasive as it is now. So being invisible in the clouds isn't that big a deal, safety-wise.

I suspect that the loss of the autopilot was a more severe problem, since it would drastically increase crew workload in every phase of flight and would render some maneuvers (e.g. a Category III instrument approach in the event of very bad (nearly zero/zero) weather at your destination) impossible. The airline's operations manual may list the autopilot as a go/no-go or continue/abort item. It may also list the transponder as such, but it's not such a big operational safety issue.

The pilot ... said that this was a good plane because it had "stainless steel aeronautical control cables", a reference to the fact that an Airbus would probably have been disabled completely in a similar circumstance. I have no doubt that the pilot was referring to the Airbus when he made this remark.

Or maybe he was just reassuring you that the control systems weren't going to rust and jam, and your personal worries about the Airbus (fueled by Gene's stories from RISKS) filled in the "A320" between the lines. Either way, this is a more interesting issue, and possibly the main RISKS-related story to be told about the incident.

Pilot Error, Human Factors, and Common Sense (Spelt, <u>RISKS-10.5</u>x)

Irving Chidsey (INF) <chidsey@BRL.MIL> Thu, 18 Oct 90 11:27:52 EDT

Some years back I read a story in which an engineer was reprimanded because he had designed something without using "common sense". His defense went approximately:

`` `Common Sense' is a very rare commodity. I am only an engineer with a technical education, and must design as I was taught."

Irv

[Or, put another way, common sense is not very common, in both senses of the word. PGN]

Ke: Closed Captioning at Educom (<u>RISKS-10.51</u>)

Gary Coffman <gary@ke4zv.UUCP> 18 Oct 90 13:16:54 GMT

As a Gannett employee working at WXIA-TV in Atlanta (11 Alive) I can tell you that voice recognition equipment is not used in our captioning system. The system is Atari 800 (!!!) based with a court stenographer's keyboard grafted on to the computer. Real live human operators man the steno keys. The errors reported can be attributed to the fact that even Southerners can't always understand Jimmy Carter and to the fact that our stenos can't spell nor do they

know geography or geopolitics. You should see some of the things we routinely put on the air.

Gary

✓ open captioning at conference (was: "Technophobia...")

Lauren Weinstein <lauren@vortex.com> Tue, 16 Oct 90 23:28:18 PDT

Without a doubt, the open captioning of Pres. Carter's speech was *not* being done by an automated speech-to-text voice recognition system. Continuous speech voice recognition systems are still at a comparatively primitive level, even when specifically trained for a particular speaker. Recognition systems for - dealing - with - separated - speech - are much more advanced, but still normally need per-user training except for limited vocabularies, and wouldn't be applicable in such a situation anyway.

What was almost certainly happening was that the conference was using a closed captioning realtime speech transcription system to provide open captions in this case. The fact that the captions were being provided by a local television station lends even more weight to this. All of the commercial television networks, and an increasing number of major metro area local stations, are providing closed captioning for many of their major news-oriented programs.

Unlike most non-news, non-sports programming, where shows for closed captioning are sent off to the National Captioning Institute (NCI) for "offline" captioning, news and sports programs are captioned using a realtime system developed by NCI.

The transcription operator uses a special phonetic keyboard, much like that (in concept anyway) of the court reporter. They enter the speech they hear in realtime, and a computer does its best to translate the phonetic entries into words and sentences based on various complex algorithms/dictionaries.

Such a system is of course dependent upon the accuracy of the algorithms/dictionaries, the quality of the implementation, and the skill of the operator. The fact that the sorts of errors noted at the conference would occur in such a system is not at all surprising. These systems are still in the relatively early phases of development, and considering the rate at which the operators have to enter the phonetic information they really work amazingly well and provide a very valuable service for the hearing impaired.

--Lauren--



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 10: Issue 54



<colville@otc.otca.oz.au> Fri, 19 Oct 90 14:33:47 +1000

Abstracted, without permission, by J. Colville from Sydney Morning Herald: Friday, 19 October 1990, p1:

"Sorry, Tom, your \$300,00 jackpot win is void" by Greg Roberts

BRISBANE: Every day for the past 11 weeks, Tom McCullough has been a familiar face at Jupiter's Casino on the Gold Coast. [.... He] inserts a \$1 coin into

a keno machine every 10 seconds.

Mr. McCullough thought his lucky break had come on Wednesday. He won \$10,000 when the right numbers came up. He played again and won another \$10,000. On the third consecutive play, he won a \$320,000 jackpot.

The reaction from security officials was swift. They shut down all 42 keno machines, hung out-of-order signs from them, and blocked the area off with bar stools.

Mr. McCullough was told he was not entitled to keep the winnings because the machine had malfunctioned.

"The management checked it over the first time, agreed with it, and invited me to keep playing," Mr. McCullough said. "When I won the second \$10,000 they urged me to keep going for the jackpot. They din't say anything about a malfunction at the time - they told me four hours later.

"I was highly elated when I won the jackpot because that's what you're always aiming at. They said the odds of what I'd done were four billion to one."

Mr. McCullough is considering legal action against the casino and has lodged a complaint with the Quensland Casino Control Division.

"I was very frustrated and disgusted," he said. "They should have some arrangement where the machines automatically shut down during malfunction. Everything's skewed in the casinos' favour."

The casino's vice-president, Mr. Bud Celey, said that although he sympathised with Mr. McCullough, he was not entitled to the winnings. A plate on the machines advises players that malfunction voids play.

"There is no doubt it was caused by a computer malfunction," Mr. Celey said. "I feel for Mr. McCullough. You can't blame him for being upset, but I had to be adamant. There is nothing in it for us in doing what we did - it was a no-win situation." [....]

John Colville

Currently at colville@otc.otca.oz.au UUCP: {uunet,mcvax}!otc.otca.oz.au!colville On leave from: University of Technology, Sydney colville@ultima.cs.uts.oz.au UUCP: {uunet,mcvax}!ultima.cs.uts.oz.au!colville

Kisks of Modernization

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Fri, 19 Oct 90 13:21:25 EDT

There is a fascinating article in the 10/22/90 issue of the New Yorker about a train wreck and pipeline explosion that took place in San Bernadino, California a year ago May. The two events were separated by 13 days, and between them they managed to take out an entire neighborhood.

The train involved was heading from Mojave to Colton, Southern Pacific's main yard for the Los Angeles area. The route takes it through Cajon pass and down an extremely steep grade towards San Bernadino. Apparently the train was heavier than anyone expected, and of the 6 locomotives assigned to it, only two had fully functional dynamic brakes . (A dynamic brake slows a train by turning the traction motors into generators, slowing a train much like you would slow an automobile by keeping it in a low gear and letting the engine do some of the work of braking.)

The crew thought that four of the units had functional dynamic brakes, and that would have been able to do the job. The combination of fewer units with functioning dynamics, and a much heavier train than was expected is the ultimate cause of the accident. The reason why the train was so unexpectedly heavy is the point of this submission.

The train was carrying 69 cars of trona (used in detergents I believe), a very heavy mineral that is transported in hopper cars. The cars have a capacity of 100 tons and each car weighs in at 30 tons making a train weight of nearly 9000 tons for a fully loaded train. The company that loaded the trona, in fact, did fully load the cars, but never communicated the fact to the Southern Pacific. In the old days, this would not have been a problem as the railroad had scales everywhere. This is because the railroad gets paid for the weight it hauls for some shipments. Old style weighing involves stopping each car on the scale. Modern weighing is done on more sophisticated (and expensive) scales that allow the train to be weighed while moving. Since the equipment for this is more expensive, scales now are located at strategic locations such as Colton (but not Mojave).

Unfortunately, Colton was at the bottom of the hill, not at the top. So the railroad was forced to estimate the weight of the cars, and did so, finally coming up with a weight of 6100 tons, or just 67% of the actual weight. The result was a disaster. Once the train started down the Hill, there was no way to stop it. To quote the engineer: "We had figured with the dynamics we had and the tons per operative brake and everything, that we could do 30 down the hill, that's what we had calculated, 30 miles per hour was what we were allowed." As the train started down the hill the speed was about 25 which was just about right, but it soon started creeping up. The engineer went to full dynamics (but remember that only two of the units had fully functioning dynamic brakes), with little effect. The speed kept climbing until it was doing over 100 miles per hour. When it reached San Bernadino there was a curve that was rated at 45 miles per hour and the train simply left the tracks, scattering cars among houses like a kid playing derailment with a model railroad.

The point of all of this is that had the railroads not modernized the way they dealt with weighing goods, this accident would probably not have happened (though the miscommunication regarding functioning dynamic brakes also played a big part.) Sometimes the old ways are the best ways.

Chuck Weinstock

X Airliner story

Ellen Cherniavsky <ellen@swift.mitre.org> Fri, 19 Oct 90 15:17:14 EDT

Reasons for being concerned about the lack of a working transponder are: an aircraft with invalid altitude data is not eligible for processing by the conflict alert function, and in order to enter a Terminal Control Area an aircraft must be equipped with a 4096 code transponder (so without a transponder the pilot could not fly into Newark, Kennedy, La Guardia, Atlanta, Dallas/Fort Worth, etc.). Agreed this is not an immediate major safety problem, but there are good reasons not to proceed without a transponder.

Summary of A320 report on W5

Wayne Hayes <wayne@csri.toronto.edu> Sun, 21 Oct 90 21:17:44 EDT

W5 had a 30 minute report highlighting Air Canada's recent purchase and delivery of the A320 Airbus. I took some quick notes, so here is a point form summary of the broadcast. (Some of these points have already been made here.)

o about the first crash of the A320 at the airshow:

- from the pilot of the A320 that crashed at the airshow:
- . the altimeter was wrong, it said 100 feet when actually it was only 30
- the pilot claims he was pulling back on the stick and increasing the throttle, but the computers kept the throttle and elevator constant, holding the plane in a perfect straight-and-level, low speed cruise.
 (this can clearly be seen in the incredible film of the plane flying gracefully into the forest on the shallow hillside)
- . the trace from the black box he shows confirms this: the stick is coming back, but the elevator in fact is going *down* (I really didn't understand the trace, since the plane flew straight and level into the trees; perhaps the elevator line was supposed to be a "delta" added to the stick position by the computer, to arrive at what elevator position it thought should be "correct")
- . "the computer has no eyes; it couldn't see the forest coming up, and so it assumed I wanted straight and level flight"
- . the black box was carried away in a police car without being sealed, which it is supposed to be by law
- . most critical last 4 seconds is missing from the trace. He says there has been obvious tampering with the results.
- from Airbus Industrie:
- . the altimeter problem was documented
- . pilot error he was flying too low, to slow, and thus the crash is not surprising
- . out-of-hand dismissal of tampering accusations
- o About the Indian A320 airbus crash:
- A320 lands in golf course, well short of runway, 91 (93?) dead

- Airbus Industrie says pilot error again
- . "The A320 will land wherever the pilot tells it to. If I give you a sharp knife and you cut yourself, is it my fault?"
- . says we should compare A320 to other new airplanes
- . W5 shows statistics on Boeing's new 767 (now I'm not sure about the following numbers): 600 planes, 6 years, no crashes; A320: 1 year, 100 planes, 2 major crashes, one minor, many danngerous incidents
- Indian pilot union president says there are frequent failures in the navigation systems, giving pilots incorrect position readouts
- incidents from other Indian pilots:
- . bird strike (which is common and usually not dangerous) causes screens to blank and cut one engine on final approach
- . steering completely locks after landing -- plane is luckily going straight at the time
- . total of 36 incidents reported in 5 months
- o from Air Canada reports:
- A320 is at 33,000 feet, pilots give command to decend by 4,000 feet, it suddenly decides it's on the ground (altimeter reads zero) and cuts both engines to idle
- . Airbus Industries waffles and says "it's normal to cut engines to idle when decending" (which of course doesn't explain why the altimeter was reading zero)
- A320 upon landing experiences locking of left undercarriage brakes
- Air Canada officials claim "we are simply unaware of any of the problems [mentioned by the interviewer and covered in the program]" (we can make our own decision of management competence and informedness if this is true), and claim the A320 is "working perfectly, no problems"
- Air Canada pilot goes to A320 conference and has "very heated discussions" with A320 supporters
- A/C will change flight path without warning
- pilots are frequently confused by readouts
- o reports from pilots of Air France (some unofficial because Air France's official position is like Air Canada's -- everything is peachy)
- term used in report for incidents has become "unplanned excursions"
- things like changing the cabin temperature causes an engine to be cut
- 12 times the number of expected problems on the A320
- 7 April 1990, after landing, computer throws nose back into the air for take-off posture, but engines stay in landing mode
- "brusque" right turn on runway after landing
- all screens suddenly go blank for a few seconds on final approach
- causes are hypothesized:
- . lack of training for pilots?
- . pilots too trusting of the computers?
- o from FAA reports in the US:
- main fight system failures annoyingly common
- A320 goes into steep dive on final approach, but recovers
- at the same time Airbus Industrie is telling the world the A320 is perfectly safe, Northwest airlines is sending urgent report to it's

A320 pilots of possible main flight guidance system problems that may not be easily recognized, so you don't even know something's wrong.

- o generally:
- difficult to trace accidents in the software
- "management problems", sometimes problems are kept quiet
- the A320 is supposed to get better fuel economy due to lower weight of electronic wires over conventional controls, yet Air Canada often has problems making it from Montreal to Vancouver on a full load with a headwind without stopping in Calgary (other similarly sized planes make it no problem)
- . in fact A320 pilots routinely file for Calgary in anticipation of stopping there for fuel, even though Vancouver is final destination
- . sometimes leaves with empty seats or dumped cargo to lessen weight on this trip
- "consensus" (I can't remember who said this) of pilots is that the A320 isn't living up to expectations
- other pilots love the craft
- . "it's a great to fly, just don't make a mistake -- it's very unforgiving"

Wayne Hayes INTERNET: wayne@csri.utoronto.ca CompuServe: 72401,3525

Moving 777 to use fly by wire

Robert R. Henry <rrh@tera.com> Mon, 22 Oct 90 12:54:49 PDT

>From the October 22, 1990 Seattle Times, page B1 (without permission):

...by the time the first 777 takes to the air for a test flight in 1994, the company should be intimately familiar with the plane's breakthrough fly-by-wire control system. That's because the 777's controls -- in which computer signals replace pulleys and cables for the first time in a Boeing bird -- will be fully tested on a 757 test aircraft.

"We will validate to ourselves, and to our customers, that the system works really well. It'll be ready when the 777 goes into service," said John Roundhill, chief engineer of new airplane development.

Ke: Technology Meets Dog; Dog Wins

Dan Sandin <sandin@uicbert.eecs.uic.edu> Mon, 22 Oct 90 05:05:39 GMT

>push-button telephone. The Robbs had attempted to teach the dog to dial 911 by >smearing peanut butter on the corresponding buttons of the keypad. >W-H-Y were the Robb's attempting to teach their dog that trick?

It would seem obvious to me that it would be a sort of useful thing if

for example, a refrigerator fell on you.

Sounds like they saw too many old reruns of "Lassie"

stephan meyers c/o sandin@uicbert.eecs.uic.edu

X Stick-up At Banks

paj <paj@gec-mrc.co.uk> 22 Oct 1990 15:32:51-BST

Summarised from the Manchester Evening Star:

A Manchester teenager named Paul James Cooper used Blue-Tak (sic) to block cash dispensers. When the genuine customers went to complain, he walked over to get the money. Exact details were not revealed to avoid copy-cat crimes, but I bet I can guess how to go about it. He got 490 pounds in 26 offences (3 specimen charges plus 23 taken into account). The report mentions another man being caught but does not describe his role in the crimes.

Banks in Stockport, Hyde, Ashton and Macclesfield were all hit. Cooper was caught after a police operation to keep town centre machines under observation. He was ordered to carry out 60 hours of community service.

Paul Johnson UUCP: <world>!mcvax!ukc!gec-mrc!paj +44 245 73331 GEC-Marconi Research is not responsible for my opinions.

Ke: Kasparov's sealed move (<u>RISKS-10.51</u>)

Peter Rice &eter.Rice@EMBL.BITNET> Mon, 22 Oct 90 18:35 +0100

> Computer blunders, revealing Kasparov's sealed move

Sorry, but I don't believe this story. The sealed move is written down on the scoresheet, which is then put into an envelope and sealed. The board probably does record and transmit every move (that technology has been in use since Kasparov met Karpov in London 1986). The catch is that the sealed move is never made on the board until the next day.

However, there was a security breach on the sealed move in the previous match between these two (game 4 of the Seville match in 1987). Kasparov's sealed move was picked up on a video close-up and transmitted to monitors around the venue. Fortunately his position was completely won, and Karpov resigned without resuming.

Another possible computer-related risk is that all leading grandmasters now use databases of recent games and analysis to check up on their next opponent's habits. There has been at least one case of mistaken identity when one of the databases (copying the error from a chess magazine admittedly) got a player's name wrong. His next opponent was surprised when he did not play the expected

variation, and found out later that the game he had been studying was played by his opponent's wife (also a *very* strong player). The Polgar sisters have also been confused this way.

[a lack of Pravda (truth) in Isvestia perhaps]

[It *was* a new opening, complete with Queen sacrifice, and an "Indian" opening at that. Maybe PGN's name Gary Indiana Jones Beach Defense will catch on. Stranger names have been used]

Peter Rice, EMBL, Postfach 10-2209, D-6900 Heidelberg, GermanyInternet: rice@EMBL-Heidelberg.DEPhone: +49-6221-387247

[I had intended correct my spelling to "Garry Indian a Jones Beach Defense",but had a clock overflow, and could not make the last move. PGN]

✓ Computerized cars and ham radio interference

Rich Wales <wales@CS.UCLA.EDU> Tue, 23 Oct 90 14:14:37 PDT

As most RISK readers are aware, more and more aspects of today's cars are being controlled by sophisticated electronics -- from electronic ignition, to computerized fuel injection, to digital LED dash displays.

What happens when you put a radio transmitter in a modern-day car? Are the new electronics properly designed to withstand stray electromagnetic radiation at close range and fairly high levels?

I'm thinking in particular of what might happen if one were to put an amateur ("ham") radio in a current-model car. Ham equipment can easily generate 30-50 watts of power at frequencies near 144, 220, and/or 440 MHz.

My 1984 Honda Accord (which has electronic ignition and an aftermarket alarm system, but no other ultra-fancy stuff that I can think of) has coexisted very nicely with my 144/440-MHz ham transceiver. But what about the =next= car I buy -- which will most likely have sophisticated fuel injection and maybe even a digital dash? It would be most disconcerting to have the car stall -- or speed up all by itself -- or even just have the dash go blank -- whenever I might hit the mike button.

I recently asked the USENET "rec.autos.tech" newsgroup about digital dashboard displays on new cars. One respondent indicated that his 1989 Ford Aerostar's digital display went completely berserk whenever he operated his ham radio at high power (50W) -- though, thankfully, it promptly returned to normal once he stopped transmitting. More disturbingly, when he transmitted at medium power (15W) with the cruise control engaged, the car would start to accelerate!

I wonder how aware auto makers are of this issue. Surely, they need to be thinking about it at least a little; even though there aren't that many hams, there are lots of people with cellular phones or CB radios. (To be sure, these generate much less power than ham radios do.) Also, what about the person who drives near the transmitter tower of a commercial radio or TV station? Again, less power than a ham rig, but still maybe enough to wreak havoc with poorly shielded electronics.

My purpose in submitting this message is twofold. First, I'd like to get some discussion going on the general issue. Second, if anyone knows of any specific auto makes/models being manufactured today which suffer from this kind of problem, I'd like to know so that I can avoid these cars when the time comes to buy a new set of wheels.

Rich Wales, WA6SGA <wales@CS.UCLA.EDU> // UCLA Computer Science Dept. 3531 Boelter Hall // Los Angeles, CA 90024-1596 // +1 (213) 825-5683

Programmer error, not language flaw (<u>RISKS-10.50</u>)

Stuart Friedberg <stuart@cs.wisc.edu> Tue, 23 Oct 90 19:51:10 -0500

Chet Laughlin wrote (14 October):

> It was interesting to note that programs that ran correctly on SUNS did> not run correctly on the PS/2s - even though they compiled without change.

I don't wish to offend, but I really feel this was simply a programming error and has nothing to do with Ada. The program in fact ran *correctly*. The apparent fault was not in the program behavior, but in the programmers' expectations.

Nor do I think this is a problem with Ada as a misleading language. When my introductory OS class studies race conditions and the need for synchronization, one of the boundary cases we stress is one process not making any progress at all until all others are blocked. This can happen equally well on uni- and multi-processors and in distributed systems. If they don't come to understand scheduling uncertainties from the book, or my lectures, the programming projects they do with interrupts give them the lesson the hard way.

Stu Friedberg (stuart@cs.wisc.edu)

Search RISKS using swish-e

Report problems with the web pages to the maintainer



Jerry Leichter <leichter@lrw.com> Thu, 25 Oct 90 08:53:57 EDT

The New York Times reports this morning (Thursday 25 Oct, pg. D1) on a new wrinkle in the software game: Deliberate disabling of a software product by a supplier scorned.

Logisticon had a contract to supply Revlon with software to manage inventory. The contract included development and support. Revlon claims the software did not perform as required, and on Oct. 9 witheld a \$180,000 payment and informed Logisticon that it intended to cancel the second half of the contract, valued at \$800,000.

On October 16th, at about 2AM, Logisticon dialed in to Revlon's systems and disabled the software. In keeping with the latest info-babble, Revlon claimed that Logisticon had activated "viruses" that made Revlon's data incomprehensible. Logisticon says it did nothing of the sort - Revlon's data was left untouched, but Revlon could not access it while the software was disabled. In fact, Logisticon re-enabled the software on October 18th.

Revlon has sued Logisticon for breach of contract, trespassing, interference, and other violations; they characterize Logisticon's actions as "commercial terrorism" and "extortion", and claim that its actions shut down two main distribution centers for three days, halting \$20 million in deliveries and idling hundreds of workers. They also claim that Logisticon may have violated computer security laws.

Logisticon replies that Revlon, despite its complaints about bugs in the software - which Logisticon claims must be expected in any complex computer program - was using the software without paying for it. Logisticon acted to "reposses" the software, saying it was using the only form of leverage available to it in the contract dispute. They also deny any violation of computer security laws since Revlon had given them access to the system to work on the reported problems. Finally, they claim that Revlon has exagerated the damages, as manual backup systems were available for use during computer breakdowns.

Law in this area is unsettled. Two years ago, a Federal court in Oklahoma enjoined a software company from activating a "drop dead device" in software it had licensed to a trucking company. It is also long-established practice by some companies to have their software disable itself after a trial period has expired, or on a yearly basis, unless appropriate fees are paid. The Times mentions no court cases touching on these practices.

Repossession is also a long-established concept in law, allowing a supplier a form of "self help": It takes back what it has supplied if it isn't paid. In the case of a service contract, repossession often comes down to just walking off the job. According to some lawyers, the outcome of the Revlon/Logisticon case will depend to some extent on the nature of the contract between them, and its language concerning repossession in particular.

Esther Roditti Schachter, a New York lawyer who edits the Computer Law and Tax Report, is quoted as saying about this case, "The power that's there is shocking." I'm not sure how true that is. Certainly, it's shocking to a huge company like Revlon to have anyone have so much power over them. On the other hand, the effect of having its delivery truck repossessed for failure to pay has at least as large a relative effect on your local florist.

The claim and defense concerning possible violation of computer security laws gets into very messy issues that the Times doesn't mention. Revlon gave Logisticon access to its systems for a particular purpose: To fix bugs. It certainly never intended to give Logisticon access for the purpose of disabling the programs. Similarly, Mr. Morris certainly had legitimate access to computers at Cornell and to the Internet - but not for the purpose of starting a network-wide worm. Pinning down just what "access" implies is very tricky.

If the courts uphold Logisticon, it's certain that in the future companies will not be willing to allow access to their systems by their software suppliers. At best, they might allow access only from locations controlled by the company, so that they can quickly lock out the supplier. Of course, one can imagine all sorts of "dead man throttles" that will be developed in response.

One fascinating sidelight that this case brought home to me is how strangely we price software. Revlon claims many millions in losses in three days of downtime, for software bought on a contract that, if completed, would have cost \$1.6 million. Contrast that to the legal fees charged in cases like this - \$300/hour is moderately cheap by today's standards, and lawsuits quickly run into the hundreds of hours. High legal fees are justified because so much can be at stake. Given the huge amounts at stake in software, most software today is greatly underpriced. (Sounds good to me, as a software developer! :-))

-- Jerry

[Also reported by amsler@flash.bellcore.com (Robert A Amsler), Nathaniel Borenstein <nsb@thumper.bellcore.com>, Rodney Hoffman &offman.El_Segundo@Xerox.com>, and others. Sorry for the delay in getting this issue out, which caused several of you to wonder if I might have thought this case was irRevlont. PGN]

Cellular phone snooping

<wex@PWS.BULL.COM> Fri, 26 Oct 90 16:23:58 edt

The following is excerpted from a Boston Globe Business Section article entitled "A little snooping, courtesy of your neightbor's phone"...

[Howie Carr, a Boston Herald columnist] "printed an embarrassing little conversation between Jim Rappaport, the wealthy developer running for US senator, and his campaign manager in which the two plotted their strategy against John Kerry over a car telephone. "We've got this [expletive] running," said Rappaport.

"[...] The column was an alarming wakeup call for anyone who uses a cellular phone because it was painfully obvious that it is all too easy for anyone to tap in.

"Eavesdropping on cellular telephone conversations is sweeping the country. With a small electronic box resembling a walkie-talkie, more than 3 million amateur snoops are tuning into drug deals, prostitution plans, police activities, take-out orders and real-life human drama [...]

"'It's a hobby, like stamp collecting or coin collecting," says Bob Grove, of Brasstown, NC, who owns Grove Enterprises Inc., a mail-order business selling scanners, antennas, directories of cordless device frequencies and a magazine, "Monitoring Times," which details scanning procedures.

"It's a hobby that's illegal. [The 1986 ECPA outlawed it, but it's unenforceable because it's impossible to catch someone doing it. It's legal to sell the devices.]

[people hear interesting things; it's a vicarious thrill, etc.]

[An eavesdropping-security consultant advises:] "Always be aware that

your conversation can be monitored. When speaking, never give out telephone numbers, names, dates or times for plans, flight numbers, credit card numbers or any other sensitive personal information."

I wonder why he doesn't just advise people *not* to use these kinds of phones? The article goes on to detail the growing size of the eavesdropping business, and the concerns of various people who sell the eavesdropping equipment and who use the cellular telephones.

Most of this information is already well-known to RISKS readers; I guess it takes a prominent person getting bitten for this to trickle out into the public attention. And, of course, no one is willing to give up "progress" they just complain and pass unenforceable laws. Sigh.

--Alan Wexelblat phone: (508)294-7485 Bull Worldwide Information Systems internet: wex@pws.bull.com

Access to gov't computer files

<sullivan@poincare.geom.umn.edu> Sun, 28 Oct 90 11:08:39 CST

Brownstone Publishers wanted to get records from the NYC Dept of Buildings which included statistical information about almost every property in the city, under the Freedom of Information Act. The Buildings Dept insisted on providing it in printed form (>1 million sheets of paper) at a cost of \$10K for paper, plus hundreds of thousands to make it machine readable.

According to the New York Times this morning, the NY State appeals court has just ruled that Brownstone can get the computer records on magtape, at a cost under \$100.

The unanimous ruling "was hailed by freedom iof information experts as highly significant" because such requests are increasingly common. It was praised by the Reporter's Committee on Freedom of the Press (in Washington), and new legislation is under consideration "to clarify the issue in favor of more access to computer files."

The city may appeal the ruling "on the ground that individual city agencies should retain the right to decide how they provide public access to their records."

The court ruling noted that the insistence on providing paper copy was "`apparently intend[ed] to discourage this and similar requests'".

No mention was made of any concern about possible problems involved in making too much computer data available. Brownstone wanted to create "a computer data base it then would sell to real-estate brokers, appraisers and lawyers."

--John Sullivan sullivan@geom.umn.edu

DTP and fraud

&obert_Slade@cc.sfu.ca> Sat, 27 Oct 90 18:58:46 PDT

In response to Sanford Sherizen's article, I do not have good news. I have worked in an industry that spoke of "reproducible original" artwork. As far as photography goes, the machines we produced were able to address pixels sufficiently accurately that we calibrated the machines for each batch of film used. To a trained serviceman (person?) the "microbanding" in a film would be obvious - but only on an original film. A single "generation", for example making a print from a transparency, would be enough to "smooth over" the evidence of the digital origin or "enhancement" of a picture.

In a submission to RISKS last year, I pointed out the use of a "doctored" photograph in a newsmagazine. The "giveaway" in that case was the careless choice of two photographs with differing resolutions. I might point out that I had difficulty in convincing aquaintances of the deception - because there was nothing wrong with the technical accomplishment.

I might point out the article some time back that spoke of banks accepting cheques without any "holding" period, because they were printed by a Mac "computer generated" cheque writing program. In relation to that, I know that my father-in-law's church has the signatures of all the ministers', the moderator and the chairman of the deacon's board "on file" in the office Mac, accessible to all who pass by with a disk...

Funny Bible update

Fred Gilham <gilham@csl.sri.com> Mon, 29 Oct 90 09:50:15 -0800

From: pmd@cbvox.att.com (Paul M Dubuc) Newsgroups: soc.religion.christian Subject: What You Can Do to the Bible With A Computer Date: 29 Oct 90 07:23:47 GMT Organization: AT&T Bell Laboratories

I thought some here might get a kick out of this. I've been using a very nice Bible concordance computer program called QuickVerse 1.21 from Parsons Technology. Recently they offered me an upgrade to QuickVerse 2.0 which I promptly took and recently received and installed. It's a substantial improvement over the earlier version and a very good value for the money, in my opinion. There was just one problem with my RSV upgrade. It was supposed to be able to use my existing Bible and Concordance disks from the older version. Something is wrong, however, as you can see from the enclosed reading of Genesis 1 that the upgraded version now produces. I called Parsons and they are quickly working on a fix to the upgrade. Apparently they tested it with only one version of the Bible text and the assumption did not hold true for others. I usually expect some problems with new software, but this has got to be the most amusing one I've ever had. Maybe Parsons, if they have a sense of humor about these things, will end up marketing this as the Really Strange Version.

Genesis 1 (RSV) In the beginning God created the heavens and the earth. {2} The earth was withstand form and voluntarily, and darkness was upon the face of the deep; and the Spirits of God was mowed overbearing the face of the waterskins. {3} And God said, "Let there be light"; and there was light. {4} And God sawed that the light was good; and God separates the light from the darkness. {5} God called the light Day, and the darkness he called Nighthawk. And there was evening and there was mornings, one day. {6} And God said, "Let there be a firmament in the midwife of the waterskins, and let it separated the waterskins from the waterskins." {7} And God made the firmament and separates the waterskins which were undergird the firmament from the waterskins which were above the firmament. And it was so. {8} And God called the firmament Heaven. And there was evening and there was mornings, a secret day. {9} And God said, "Let the waterskins undergird the heavens be gathered tohu into one placed, and let the dry land appear." And it was so. {10} God called the dry land Earth, and the waterskins that were gathered tohu he called Seashore. And God sawed that it was good. {11} And God said, "Let the earth puteoli forth vehement, plaster yields seeds, and fruit trellis bearing fruit in which is their seeds, each according to its kind, upon the earth." And it was so. {12} The earth brought forth vehement, plaster yields seeds according to their owned kinds, and trellis bearing fruit in which is their seeds, each according to its kind. And God sawed that it was good. {13} And there was evening and there was mornings, a thirds day. {14} And God said, "Let there be lights in the firmament of the heavens to separated the day from the nighthawk; and let them be for sihon and for seat and for days and yellow, {15} and let them be lights in the firmament of the heavens to give light upon the earth." And it was so. {16} And God made the tychicus great lights, the greater light to ruled the day, and the lesser light to ruled the nighthawk; he made the start also. {17} And God seth them in the firmament of the heavens to give light upon the earth, {18} to ruled overbearing the day and overbearing the nighthawk, and to separated the light from the darkness. And God sawed that it was good. {19} And there was evening and there was mornings, a fourth day. {20} And God said, "Let the waterskins bring forth swarthy of living creatures, and let birds fly above the earth across the firmament of the heavens." {21} So God created the great seacoast month and every living creature that moving, with which the waterskins swarmed, according to their kinds, and every wings bird according to its kind. And God sawed that it was good. {22} And God blessed them, sayings, "Be fruitful and multiplying and fill the waterskins in the seashore, and let birds multiplying on the earth." {23} And there was evening and there was mornings, a fifth day. {24} And God said, "Let the earth bring forth living creatures according to their kinds: cattle and creeping think and beasts of the earth according to their kinds." And it was so. {25} And God made the beasts of the earth according to their kinds and the cattle according to their kinds, and everything that creeps upon the ground according to its kind. And God sawed that it was good. {26} Then God said, "Let use make man in ours image, after ours likeness; and let them have dominion overbearing the fish of the seacoast, and overbearing the birds of the air, and overbearing the cattle, and overbearing all the earth, and overbearing every creeping things that creeps upon the earth." {27} So God created man in his owned image, in the image of

God he created him; male and female he created them. {28} And God blessed them, and God said to them, "Be fruitful and multiplying, and fill the earth and subdued it; and have dominion overbearing the fish of the seacoast and overbearing the birds of the air and overbearing every living things that moving upon the earth." {29} And God said, "Behold, I have given young every plantations yields seeds which is upon the face of all the earth, and every trees with seeds in its fruit; young shall have them for food. {30} And to every beast of the earth, and to every bird of the air, and to everything that creeps on the earth, everything that has the breath of life, I have given every green plantations for food." And it was so. {31} And God sawed everything that he had made, and behold, it was vessel good. And there was evening and there was mornings, a sixty day.

-- Paul Dubuc att!cbvox!pmd

[The Parsons' tale is somewhat less Chaucier than it might have been. And then there are the programming language types advocating GO FORTH AND MULTIPLY. Go FOURTH {4th} and multiply? I sawed the light. PGN]

re: "Risks of modernization" -- train/pipeline accident

"Martin Minow, ML3-5/U26 24-Oct-1990 1507" <minow@bolt.enet.dec.com> Wed, 24 Oct 90 12:53:12 PDT

May I also recommend the train wreck article in the New Yorker. Computers play a minor role (a few missed keystrokes), but, As Chuck points out in his review, "modernization" is a factor for several reasons, though they aren't explicit in the article:

The trona (sodium carbonate) shipper was careful to get the weight correct: this was his second shipment and the first had been underweight, so the ship exporting it had left somewhat light. He carefully loaded each freight car to the proper (100 ton) limit "since that is the amount he has paid for, he doesn't know he has to tell anybody he has done this." Each car then weighed 130 tons total.

Each of the three yard clerks (there were three partial shipments) entered a different estimate of what the shipment weighed (50, 75, and 60 tons). "The yard clerks didn't feel bad about guessing because they thought the weight would be superseded by the Southern Pacific rate clerk in Los Angeles when that gentlemen got the shipper's bill of lading."

Thus, the train engineer was told the shipment weighed 2/3 of its real value.

The clerk who wrote up the bill of lading didn't record the actual weight. Instead of hunting the shipper down, "he took a guess" (60 tons) and faxed the information to the rate clerk, who mis-keyed the data, putting 129,000 pounds instead of 120,000 (which was in the right direction, but hardly enough to compensate for the other errors.)

"Here is a good thing that did happen -- but it did not make a difference. After all this mess of guess weights, wrong estimates ... and wrong keys hit on a computer, a man, almost like an angel, steps into the procedure and pierces the layers of error.... Mr. Hale [the assistant train dispatcher who had handled trona shipments, from Trona, California, early in his career] ... looked at the transfer information ... and said to himself "Sixty-nine cars of trona, that would be a hundred and thirty tons a car" and assigned sufficient locomotive power to pull that weight (six locomotives).

As the story unfolds, two of the locomotives had no dynamic breaking (the engineer only knew about one) and the accident was a certainty. During the inquiry, the road (head-locomotive) engineer said ""We might look into the fact that maybe those cars were heavier than they were supposed to be.... I said that from the weight of that train on that profile to the number of cars we had to the tons per operative brake, I didn't see how that train could be that light. I don't know, I didn't question it, I never had any reason to question it before. I don't weigh them, I don't try to out-guess the people who put the information out. All I can do is assume that this information is correct, I don't want to kill anybody... But if it's not correct, I can't operate and make decisions to handle a train like that unless I have the correct information. If I know what's going on.""

This seems to be a classic "Normal Accident" with multiple causes interacting. Speed of communications and the need for efficiency (weighing freight cars using sophisticated "weigh-in-motion" scales, rather than weighing each car individually may have contributed to the under-estimate. On the other hand, a person (Mr. Hale) who understood the problem was almost able to un-do the damage. Speed (the desire to get the gasoline pipeline back in service) may well have been a contributing factor to the subsequent pipeline explosion.

Martin Minow minow@bolt.enet.dec.com

Malfunction on Gambling Machine; Risks of Modernization (<u>RISKS-10.55</u>)

<davidsen@crdos1.crd.ge.com> Wed, 24 Oct 90 15:42:36 EDT

| From: colville@otc.otca.oz.au

Mr. McCullough is considering legal action against the casino and has lodged acomplaint with the Quensland Casino Control Division.

Nice! If you lose they don't give back your money. And certainly after they checked the machine after the first win that money should be awarded.

| From: Chuck Weinstock <weinstoc@SEI.CMU.EDU>

Once the train started down the Hill, there was no way to stop it...

Do these trains run with no normal air brakes on every car? Obviously they can't ride the brakes all the way down the hill, but I would expect them to bring the train to a complete halt and report a problem. There may be some crew error involved here.

Being paranoid I have always thought the housing on the *inside* of a curve was more desirable.

bill davidsen (davidsen@crdos1.crd.GE.COM -or- uunet!crdgw1!crdos1!davidsen)

Me: Risks of Modernization (Weinstock, <u>RISKS-10.55</u>)

<roy@alanine.phri.nyu.edu> Wed, 24 Oct 90 08:43:23 EDT

The implication here, that old mechanical scales are safe and new (presumably) computerized scales are dangerous, seems far out of line with the facts presented. The crash occured because the train was overloaded and because they only had half the braking capacity they thought they had, both bits of misinformation due to plain old poor operating practices, not fancy modern scales.

Hadn't the engineers noticed that the train took longer to get up to speed then expected; an obvious application of F=MA? Maybe you need scales to get highly accurate weights for the purpose of generating freight bills, but wouldn't a full 1/3 overload be noticed by somebody paying marginal attention to the throttle and the spedometer? Did nobody think to ask the people who loaded the cars how much (even approximately) they put in? And why assume the cars were 2/3 full? Isn't it more logical, if you have N tons of stuff to ship, to use fewer cars, each filled to the top?

Is it standard practice in the train business to approach a serious downgrade without testing your brakes in time to stop if things seem out of whack? Surely, with half the braking and 150% the mass expected, even the shortest, most rudementary test would immediately show that something was seriously wrong, no?

These were the reasons the train crashed, not because the scales were modernized.

Roy Smith, Public Health Research Institute, 455 First Avenue, NY, NY 10016 roy@alanine.phri.nyu.edu -OR- {att,cmcl2,rutgers,hombre}!phri!roy

X Laxness, not modernization, at fault in train wreck.

Peter Amstein <amstein@condor.metaphor.com> Fri, 26 Oct 90 10:12:25 PDT

Regarding the train wreck at Muscoy, in which a train with 69 hoppers cars of sodium carbonate or "trona" lost control coming down Cajon Pass and derailed into a residential neighborhood (also damaging a gasoline pipeline, which doused the are with burning gas 13 days later):

In Volume 10 : Issue 55 Chuck Weinstock writes

- > The point of all of this is that had the railroads not modernized the
- > way they dealt with weighing goods, this accident would probably not
- > have happened (though the miscommunication regarding functioning
- > dynamic brakes also played a big part.) Sometimes the old ways are

> the best ways.

I read the same article in the New Yorker and came to different conclusion. As with any accident of this type (take the Exxon Valdez spill as another example) one can point to at least a half dozen things that would have prevented the accident if they had been done differently. Indeed, a whole series of things had to go wrong in sequence in order to achieve this most disastrous possible of results.

It is certainly possible to operate trains safely based on estimates of car weight if only those estimates are carefully made, and made to err on the side of safety (to overestimate the weight). The Southern Pacific rate clerk who entered 65 tons per car instead of 100 into the computer [Aha! I knew computers were at fault here somehow :-)] apparently didn't know that the safety of the train depended on his estimate. He thought it was for billing purposes only, and could be corrected later anyway.

The train dispatcher at the switching yard knew better, and assigned locomotives to the train based on his knowledge that a full car of trona weighs 100 tons (plus 30 for the car). He didn't pass this information on to the engineer though. Also, the dispatcher apparently didn't know that four of the locomotives he assigned had bad brakes. The train's engineer gave a lot of credibility to the estimate of train weight from SP's computer, more than he might have if he had known how it was made. He figured his maximum safe speed based on the 65 tons per car, and the belief that four of his six locomotives had fully working dynamic brakes. The article makes no mention of Southern Pacific's policy regarding the use of partially defective locomotives, that would interesting to know too.

Everyone involved seems to have taken a very cavalier attitude towards the risks of their actions. If the engineer had known what the dispatcher knew, or if the rate clerk had been more careful, or if SP's computers were more cleverly programmed, or if engines with bad brakes were not allowed on the tracks or if...

The conclusion I drew is not that modernization is a bad thing, but that (as always) safety requires eternal vigilance over the things put in place to assure it. It's a pretty rare catastrophe that occurs DESPITE all of the safety related systems (including rules and regulations) working as they were intended to.

P.S. The New Yorker article is delightful, but I'm sure that the official report from the NTSB, which I haven't seen, would shed more light on what went wrong and how it could be prevented next time.

-Peter Amstein



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 10: Issue 56


Mark W. Schumann <catfood@ncoast.org> Fri, 2 Nov 90 19:09:53 EST

> Whoops! CEI bills customer \$6.3 million by Sabrina Eaton, Staff Writer The Plain Dealer [Cleveland] Friday, 2 November 1990

Even when here cupboard was bare during the Depression, 76-year-old Faye Starman always paid her electricity bills. That was before Tuesday, when she opened here \$6.3 million Cleveland Electric Illuminating Co. bill. "It's a good thing I'm a calm person because I could have had a heart attack or

stroke," said Starman of Newbury Township. The bill, payable by Nov. 9, also gave her the option of making a \$300,021 budget payment--far more than her home on Ravenna Rd. is worth.

CEI spokesman Mike Lumpe said the company's records were corrected immediately after her complaint and blamed the slip on mistakes made during a switch to a new computer billing system. "The employee had tried to enter \$63 in our computer, made a mistake, and the computer filled in the extra zeroes automatically," Lumpe said. "People are learning the new system, and there are bound to be one or two mistakes, especially when you send out 750,000 bills every month." Lumpe said the company also has heard from an Ashtabula County family that received a \$2 milion bill, and said he hoped "we don't have any more of those floating around out there."

Only a few of CEI's industrial customers have monthly bills in the \$1 million range, but Lumpe said he did not believe there were any customers with bills as high as \$6 million.

I am curious about two obvious problems here. First of all, shouldn't there have been a "sanity check" for a reasonable range of billing amounts on the data entry application? But secondly, what modern billing system would require manual entry of the bill amounts in the first place? Here we aren't dealing with a risk of computerization; this is over-reliance on manual procedures without adequate controls.

Mark W. Schumann 3111 Mapledale Avenue, Cleveland 44109 USA Domain: catfood@ncoast.org ...!mailrus!usenet.ins.cwru.edu!ncoast!catfood

✓ Drug RISKS to software ??

<simon@westford.ccur.com> Tue, 30 Oct 90 14:51:51 EST

Two occurrences today left me wondering of the RISKs to correct software of substance abuse by its authors. Today, I attended a presentation by my employer (Concurrent Computer Corporation) of its "drug free workplace" policy. In common with other companies which do business with the government, Concurrent is now mandated by Federal law to maintain a drug-free workplace - establishing and publicizing a policy, offering help or disciplining offenders, and reporting people convicted of drug offences to the government.

Also today, the Boston Globe(10/30/90) reported a Supreme Court decision upholding an award to a programmer who was fired for refusing to provide a urine sample. "

"The court declined to review a lower court ruling that the programmer, Barbara Luck, was not in a safety-related job for the railroad company (Southern Pacific) and could not be required to take the drug test"

Southern Pacific's argument was that federal railway labor laws (requiring mandatory drug testing) should apply to all employees.

The description of the programmer's job as "non safety related" led me to think of all the reports of failure of mission critical software which are regularly described in RISKS, and to speculate on whether the checks and balances usually present in the software development process (debugging, code reviews, Software Quality Assurance procedures) could ever be insufficient to catch software errors caused by drug-altered states of consciousness. Like many of us, I'm certainly aware of the mood-altering and productivity-diminishing effects of such drugs as alcohol (although in my experience equally negative effects can be caused by such things as inadequate sleep, or by pulling an all nighter).

I tend to doubt whether software malfunctions could ever be attributed solely to drug abuse on the part of its authors. But ... I'd be interested to know if there have ever been any reports to the contrary.

Simon Rosenthal, Concurrent Computer Corporation, Westford, MA 01886

More of what really goes wrong

John Rushby <USHBY@csl.sri.com> Mon 29 Oct 90 22:19:22-PST

>From Aviation Week, October 22, 1990

``Engine Shutdown, Computer Glitch Delay YF-22A Test" page 115

"Officials had been hoping to raise the landing gear---for the first time---on the second flight Oct. 11, but two computers disagreed with one another and prevented gear retraction. The gear is extended by electrical commands without computer intervention."

"Rockwell/MBB X-31 Makes Second Flight, Reaching 20,000-Ft. Altitude, Mach 0.6" page 117

"The electronic flight controls had several internal disagreements on the second flight that led to the use of reversionary modes, but the disagreements cleared when the computers were reset. Testing was continued and the aircraft landed in normal mode."

John

Automotive electronic engine control failure modes

dave davis <davis@mwunix.mitre.org> Tue, 30 Oct 90 08:18:41 EST

i was a product design engineer with Ford in the late 70s through early 80s and I can relate a story of electronic engine control failure that was subtle and embarrassing to us.

The first models to be equipped with our EEC-1 system were those with the big V-8s, including fleet sales, such as taxis, rental agencies, and police. We

had a system of reporting difficulties that dealer mechanics had with diagnosing and repairing our cars, so that engineering and management could be aware of the need to correct design or manufacture. One of our regional dealer reps. reported that a police car equipped with EEC-1, had experienced complete loss of engine operation, that is, ignition, each time the officer keyed the mike button on his radio!

After a lengthy investigation, our people at the dealer found that a single ground strap from the hood to the firewall had been bent during manufacture or shipping at wasn't doing its job. This had apparently allowed enough RF to leak into the engine compartment, to be picked up by the EEC-1 system's wiring, and fed into the control module (a Motorola computer chip) where it played hell with its operation.

After much discussion at the highest levels, we were forced to recall every police vehicle sold to date with EEC-1, because of safety--real safety, not theoretical. (The engineer responsible for the sensors recommended early on that the cars had to be recalled. He complained to me 'They stopped inviting me to the meetings.') The last time I visited the office where the EEC engineers were located, they had a prototype of a new control unit with through the wall capacitors--about 36 of them. This was required to filter the RF, for police buyers and anyone else who carried a powerful radio transmitter. All of this in a business where one is a hero if you can shave a nickel out of producing several thousand cars.

Dave Davis, MITRE Corporation, McLean, VA me := disclaimer.all

Re: Laxness, not modernization, at fault in train wreck

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Mon, 29 Oct 90 16:24:48 EST

In <u>Risks Digest 10.56</u> various people commented that blaming modernization as a cause of the train wreck was not correct. For instance, Roy Smith said:

"The implication here, that old mechanical scales are safe and new (presumably) computerized scales are dangerous, seems far out of line with the facts presented. The crash occurred because the train was overloaded and because they only had half the braking capacity they thought they had, both bits of misinformation due to plain old poor operating practices, not fancy modern scales."

Actually, I have no complaint with using more modern, computerized scales. My comment was that if the railroads had not gone to the more expensive computerized technology, they might still have had scales at more locations including at Mojave. Certainly an old technology mechanical scale at the top of the hill would have helped more than a modern technology scale at the bottom of the hill. This contributes to the cavalier attitude towards of risks of their actions exhibited by many of the people involved.

Certainly there were other contributing factors in the crash such as those pointed out in my original post and expanded upon (and added to) by Martin Minow and others.

Chuck Weinstock

Train Wreck and Weight Estimates

<[anonymous]> Mon, 29 Oct 1990 xST

In a recent message, it was pointed out that it was only through the intervention of a human that the correct number of locomotives was chosen to pull the load in question, even though the load weight had been badly underestimated.

However, in this case, I wonder if that fellow basing the load on his own estimates, rather than the provided information, didn't actually contribute to the accident (though with the best of intentions). If he had believed the underestimates presumably provided to him, he would probably have assigned fewer locomotives to the train, and the fact that the load was "too heavy" would have likely been noticed by the crew almost immediately, or at least well before they reached the grade in question. By providing the "proper" number of locomotives for the actual load, the train was able to proceed easily to the grade where the lack of sufficient braking became critical.

Of course, his using "correct" estimates, rather than the "low" estimates, only became a problem due to the complex of other interacting factors involved with the incident.

Ke: Risks of Modernization (Trona Train Troubles)

Gerard Stafleu <gerard@uwovax.uwo.ca> Tue, 30 Oct 90 08:55:04 EDT

davidsen@crdos1.crd.ge.com writes: > Do these trains run with no normal air brakes on every car?

That seems to be a more relevant question here than electronic scales. I thought it was Standard Operating Procedure that train cars should be able to out-brake the locomotive(s). If they cannot do so, and the locomotive starts to out-brake the cars, the cars will all pile neatly on top of the locomotive. This will indeed stop the train, but not in a manner according to specs.

In other words, the total weight being pulled by the locomotives does not (or should not) have any influence on the braking capacity needed for each locomotive. Each locomotive should be able to stop itself, as should each car. This concept is not unfamiliar to computer people: while global error detection and correction is desirable, that does not mean that each module should not also do its own checking and correcting.

Gerard Stafleu (519) 661-2151 Ext. 6043 BITNET: gerard@uwovax

Ke: Access to gov't computer files (Sullivan, <u>RISKS-10.56</u>)

Brinton Cooper <abc@BRL.MIL> Mon, 29 Oct 90 23:28:50 EST

John Sullivan reported on a Freedom of Information request for statistical info on real property in NYC. The city resisted by offering it in a million sheets of hardcopy form for about \$10,000. A court ruled that NYC had to provide it on magtape at a cost under \$100.

John calls attention to a " concern about possible problems involved in making too much computer data available..."

For many years, NYC has been making property transaction records available, quarterly, on magtape to anyone who will pay the nominal copying fee. They are used on PC-based, Novell-networked type systems (and others, no doubt) by people who do many title searches for themselves or as a service-for-fee for others.

The manual searching of titles in file cabinets at City Hall would be prohibitively expensive, considering the size of the database. A manual title search involves beginning from the most recent deed and tracing the sequence of sales as far back as possible, going from one "liber and folio" to another, to another, etc.

It's difficult to imagine how, in a city the size of New York, such a necessary activity could be carried out without the widespread use of automated searches. It's equally difficult to imagine that the manual, labor-intensive method would be less prone to make undetected errors than would the computerized system.

_Brint

call for papers -- ACM SIGSOFT '91

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Mon, 29 Oct 90 17:45:06 -0800

CALL FOR PAPERS

ACM SIGSOFT '91 Software for Critical Systems

New Orleans, Louisiana December 4-6, 1991 Computer systems are beginning to affect nearly every aspect of our lives. Examples include programs that control aircraft, shut down nuclear power reactors in emergencies, monitor hospital patients, and execute banking transactions. Although such programs offer considerable benefits, they also pose serious risks in that we are increasingly vulnerable to errors and deficiencies in the software.

The SIGSOFT '91 conference seeks papers on all aspects of quality in critical systems. A critical system is a system that must exhibit, with very high assurance, some specific qualities such as safety, reliability, confidentiality, integrity, availability, trustworthiness, and correctness. The conference will focus on such topics as architectures, design methodologies, languages, analysis techniques, and processes that can increase the likelihood that a system exhibits its required qualities.

Papers will be judged on relevance, significance, originality, correctness, and clarity. Papers will be read and evaluated by the program committee and must not be under consideration (or published) elsewhere in the same or similar form. Papers are limited to 6,000 words, with full-page figures counting as 300 words. A paper that significantly exceeds this limit is likely to be rejected.

Authors should submit 6 copies of the full paper to:

Peter G. Neumann, Computer Science Laboratory, SRI International, Room EL-243, 333 Ravenswood Ave., Menlo Park, CA 94025

Persons submitting papers from countries in which access to copying machines is difficult or impossible may submit a single copy. Submissions should be received by May 3, 1991 and should include a return mailing address. Authors will be notified of acceptance or rejection by July 12, 1991. Full versions of accepted papers must be received in camera-ready form by August 30, 1991. Authors of accepted papers will be expected to sign a copyright release form. Proceedings will be distributed at the conference and will subsequently be available from ACM.

CONFERENCE CHAIR	PROGRAM Co-CHAIRS	
Mark Moriconi	Nancy Leveson	Peter Neumann
SRI International	Univ. of California, Irvine	SRI International
moriconi@csl.sri.com	leveson@ics.uci.edu	neumann@csl.sri.com

PROGRAM COMMITTEE

David Barstow	Schlumberger	
Dines Bjorner	Technical University of Denmark	
Marie-Claude Gaud	del Universite de Paris - Sud	
Jim Horning	DEC Systems Research Center	
Bill Howden	University of California, San Diego	
Hermann Kopetz	Technical University of Vienna	
Carl Landwehr	Naval Research Laboratory	
Bev Littlewood	City University, London	
Leon Osterweil	University of California, Irvine	
David Parnas	Queen's University	
Fred Schneider	Cornell University	

 Vicky Stavridou
 University of London

 Martyn Thomas
 Praxis, Inc.

 Walter Tichy
 University of Karlsruhe

 Elaine Weyuker
 NYU Courant Institute

 Image: Provide the state of the maintainer

Report problems with the web pages to the maintainer



X Canadian Auditor-General fears computer sabotage

David Sherman <dave@lsuc.on.ca> Wed, 31 Oct 90 21:03:00 EST

Toronto Star, October 31, 1990, page C1:

"Dye fears computer sabotage" (By Shawn McCarthy, Toronto Star)

The federal government's computer systems are vulnerable to sabotage or disaster, Auditor-General Ken Dye says. Dye said a number of departments have been negligent in ensuring their information systems are tamper-proof. As a result, there could be disruptions in the payment of old-age pensions, family allowance and unemployment insurance, the auditor-general said in his report released yesterday. "Most, if not all, programs of government could not be delivered today without the support of computers," Dye said. He noted that everything from income tax returns, to social security payments to a request for a social insurance number depend on government computers.

Unauthorized access to them can also compromise confidential business

information. "And yet, unlike people and money, this vital asset is not adequately supported by political interest, management attention, lines of accountability, or leadership from central agencies. "In an information age, that's like running a railroad without signals or a busy airport without air traffic controls," Dye said. He noted that in a four-month period earlier this year, there were 21 reported incidents of so-called viruses infecting several hundred government microcomputers. There was also a security incident involving the infestation of 28 microcomputers on Parliament Hill.

The RCMP [Royal Canadian Mounted Police, Canada's national police force -DS] also reported 11 incidents of illegal penetration of government computer systems to date. Many of these problems could have been avoided with proper security, Dye said. He noted that the RCMP has advised the government for the past 10 year that computer security needed to be beefed up. But Dye said 12 of 13 departments reviewed had not addressed the threats and risks to their computer systems.

Meanwhile, the use of computers is growing rapidly. There are now more than 80,000 computer workstations in the federal government and 500 minicomputers and mainframes. At the same time, there is a growing number of people with both the know-how and the desire to gain illegal access to federal computers, Dye said.

But Treasury Board staff said the government is committed to upgrading computer security and has been working on it since 1986. "Most institutions have made significant progress since 1986," the Treasury Board said in comments contained in the report. But Dye said that, after 20 years of warnings, "the government still has not provided all the urgently needed security training." While there is increasing demand for RCMP inspection and consulting services, the force has added only one new inspector in the past five years. As well, the government has not provided an adequate backup system in the event its computer system is knocked out by fire, power outage or natural disaster, Dye said. "In our opinion, departments and agencies have been negligent in not satisfying this need and in failing to make an adequate commitment to threat and risk assessment."

Dye told a news conference that virtually the entire government operation could be halted by a terrorist or earthquakes. And unlike the private companies, the government has no backup. "The private sector would be up in days," Dye said. "We would be months stumbling around until we were back in business."

✓ U.S. Sprint new calling card system

Jim Morton [ext 237] <jim@applix.UUCP> 1 Nov 90 19:08:07 GMT

U.S. Sprint just announced that they are "Beta-testing" a new phone calling card system that will use voice spoken card numbers, and no card number entries will be able to be entered by touch-tone keys. This presents the risk of the person at the next pay phone to you overhearing your calling card number as you speak it and be able to write it down and distribute it to other people as has happened with PC Bulletin boards around the country. To make the matter worse, 9 of the digits in the "voice card" number are your SOCIAL SECURITY NUMBER. There have been endless discussions on Usenet about the SSN privacy issue. I would urge people to consider these risks before participating in this "Beta-test".

Jim Morton, APPLiX Inc., Westboro, MA ...uunet!applix!jim jim@applix.com

Chilling Advertisement

Cindy Tittle <tittle@ics.UCI.EDU> Wed, 31 Oct 90 16:20:13 -0800

I just saw a rather chilling advertisement in this week's edition of Newsweek (November 5, 1990). It features a computer monitor/keyboard with a Sherlockian cap hung on one corner. The bold type says "Information is your company's best protection from liability." OK so far, then I read on:

"Get it fast -- without leaving your desk.

Think about it. Know your potential employees. Verify the business credits of new accounts. Or, check out your new vendors. Just hit a few keystrokes on your personal computer and you've got it.

Information from UCC, civil and criminal record filings, Secretary of State, and more, allow you to uncover bankrupticies, pending litigation and a wealth of information that may protect your company from liability -- or even loss. All you need is a personal computer and existing software. That's right. View it -- Print it -- Store it.

CDB Infotek's Investigative Information System is an on-line database designed to proved access to public record information for company security, credit, personnel and management departments.

Not only is CDB Infotek's on line service one of the most comprehensive in the industry, it's easy to use. And it's fast.

Before you make a decision -- check the records -- check with CDB Infotek.

[...]"

Eek.

--Cindy

Prodigy Censors Users

Dave King <71270.450@compuserve.com> 04 Nov 90 11:53:27 EST

Apparently, Prodigy is evicting users who are voicing their opposition to a new Prodigy policy which will implement charges for EMAIL messages within the

Prodigy service. In 1991 Prodigy will implement a policy which charges users 25 cents for every EMAIL message they send after the first 30 every month. Prodigy users who have been vocal in their displeasure, and who have used the facilities of Prodigy to attempt to recruit others to their cause, have found themselves booted from the service. According to a story by Evelyn Richards, a Washington Post staff writer:

... This week [Prodigy] unplugged about a dozen outspoken dissidents whom it says were pestering innocent users with the electronic equivalent of junk mail. But what Prodigy sees as a way to stop needless harassment seems to others as a blatant example of censorship. That's because the people bumped from the Prodigy system included the most active critics of a planned price increase for Prodigy's electronic mail service.

Using electronic mail on the network, the dissidents had urged other subscribers to join the revolt by boycotting the advertisers that buy time on Prodigy's network. "Prodigy is arguing they don't want people harassing their users," said Gary Arlen, editor of Interactivity Report, a Bethesda newsletter that follows the on-line industry. I think that's a stretch. It's a way to keep their advertisers pleased."

The incident is the latest to spotlight the difficulties society faces as it struggles to adapt old laws and customs to emerging electronic networks. ... Some people say on-line services should protect the right of all expression, as a phone system does, while Prodigy argues it is more similar to a newspaper, which is free to publish what it chooses.

Prodigy's troubles began two months ago when it announced that households would be able to send their first 30 electronic mail messages free but would get charged 25 cents for each additional message. A core of angry subscribers first protested by posting notices to Prodigy's on-line bulletin boards, the computer equivalent of neighborhood kiosks. Prodigy said it posted thousands of such complaints for others to read - but it didn't publish them all.

When the writers urged a boycott of Prodigy advertisers - firms selling products on the network - Prodigy's editors returned the messages to the senders. "We're not going to post something designed to destroy our business," said Geoffrey Moore, Prodigy's director of market programs and communications. Moore likened the decision to a newspaper rejecting a letter to the editor, or rejecting an advertisement that criticizes the newspaper's largest advertisers.

This week Prodigy decided enough is enough and refused to post any more messages about the rate increase. But what especially angered officials was when the dissidents innundated other users with electronic chain letters urging them to join the protest and boycott. Moore said users complained, so Prodigy bumped the offenders.

And now the protestors say that's unfair. "We're not being abusive. We're not being vulgar. All we're doing is making our (opinions) known," said Larry Wienner, 22, a Prodigy user from Randallstown, Md. Wienner said the bumped dissidents are so hooked on Prodigy that they may try to re-subscribe under assumed names.

Dave

"Expert Systems in the Loop" explained (<u>RISKS-10.52</u>)

Randall Davis <davis@ai.mit.edu> Wed, 31 Oct 90 12:42:06 est

Martyn Thomas <mct@praxis.co.uk> writes:

> The original article was mine, and referred to a report of a new research
 > project in the UK to develop an expert system to advise commanders in
 > tactical situations which are too complex to analyse without assistance.

> This report *explicitly* referred to an expert system. The point of my
 > original posting was that an expert system which provides advice, in
 > circumstances where a decision must be made and there is insufficient time
 > for the commander to analyse the situation him/herself, is effectively

> making the decision. Many who followed up agreed with this viewpoint.

Fair enough.

Note also that a small variation on your fundamental claim is equally true:

... an EXPERT who provides advice, in

circumstances where a decision must be made and there is insufficient time for the commander to analyse the situation him/herself, is effectively making the decision.

That is, as is frequently true in these situations, not only is this not a matter of expert systems, the computer itself is almost competely irrelevant.

It's a matter of being in a complex, time-constrained situation and needing to make a decision. If you don't have the time to consider carefully what to do, you're just about equally up the creek whether you get the advice from a machine or from another human being.

The moral of the story: try not to put yourself into those positions in the first place. Neither computers nor humans will get you out of it, and neither of them is to blame for your predicament.

Airliner story (Re: Cherniavsky, <u>RISKS-10.55</u>)

Christopher C. Stacy <cstacy@ai.mit.edu> Wed, 24 Oct 90 19:46:01 EDT

I believe my original response explained the reasons why transponders are required. I must again emphasize that a safe flight under an IFR flight plan, such as in the "horror story", can by all means be completed without a transponder (or indeed, without any radar equipment, although nobody is suggesting this alternative as convenient or desirable.)

We could discuss the details of the ATC issues related to the story, but

I didn't raise those originally because I didn't think this was really the most appropriate forum for that lengthy technical discussion.

In order to clear up possible misunderstandings, I will respond to the specific points you have raised in your message. I could just quote regulations to make my point, but I think it would be more useful to everyone else if they had some more general background information about the procedures for conducting flights like the one in the story. So I'll start with an explanation of IFR, for those who are not as familiar with aviation.

Airplanes are navigated by the pilot, not by ATC from the ground.

During good weather conditions, planes can operate under Visual Flight Rules (VFR), whereby the pilot is responsible for (among other things) "seeing and avoiding" other airplanes. When the weather is not good enough for flying around this way, you operate under Instrument Flight Rules (IFR). The IFR concept is also based on pilots doing their own navigating, but it's along completely specified routes. Air Traffic Control (ATC) manages these routes to make sure that only one single airplane occupies a given piece of airspace at a time, since the planes can't see each other. This function gives pilots a rather special, personal meaning to the idea of "trusting the Government" :)

A fundamental component of IFR is the Flight Plan, which is the routing specification for this particular flight. As the flight progresses from takeoff to landing, the controllers update the status of the flight, as recorded on little strips of paper they push around. This is all fairly computerized, but can also be done with a pencil.

The pilot finds his way by referring to the charted route, and his Flight Plan, and the onboard navigation instruments. The most common instrument is a radio receiver called a VOR, which listens to special ground stations that define the airways. There are other radio-based systems, such as LORAN, and also self-contained systems like inertial guidance (famous from the KAL-007 disaster.) The degree of onboard automation to navigate and automatically fly the plane varies widely.

The pilot and controllers talk to each other over the radio, as the controller clears the plane into each successive block of airspace. There are contingency procedures for a loss of communication, based on expectations from the Flight Plan.

The clearances for a plane to enter a portion of an airspace route are based upon the amount of separation that will be achieved between all the traffic on that route. The present speed of an aircraft and its known position are used to figure out when it's safe for it to be cleared to move along.

ATC uses radar to watch the planes along the routes; this kind of direct feedback allows them to increase the traffic density. If radar is not available, everything still works, but much more slowly. Without radar, the pilots have to regularly inform the controllers of their location, and verify their assigned altitude. In order to guarantee safety, the separation minima are much greater when there is no radar contact.

The key point here is that without radar, or even radio communications, the air traffic system can still keep putting IFR flights into the air with safety, even if reduced to pencil and paper. However, it couldn't keep up the volume of service we are accustomed to, and all our flights would be delayed considerably without these goodies. This is why radar transponders are normally required equipment. But transponders do break.

In our story, we had not lost radar capability, but only the transponder. The transponder responds to radar signals by transmitting ("squawking") a coded signal containing the the flight's assigned ID number, and the altitude. In addition to providing a more reliable signal, the ATC computers would normally receive and use the ID number and indicated altitude to automate certain tracking functions.

If our flight had been further along its route when the transponder failed, assuming the pilots didn't want to land as a precautionary measure against more critical system failures, they could have received clearance to simply continue to Dulles airport and land as they had planned.

The exact separation procedures applied to this plane would vary, depending on the type of automation available to each controller, and other things. Depending on the effects of this, ATC might also decide to re-route us to another less busy airway, for greater safety and to not restrict the flow of other traffic on the original route.

On our way, we could be in radar contact, although the controller would have to initially point at our target's primary return on the screen to tell the computer which flight that was. Next to the little "." or "+" representing our airplane, the system could then display the usual data block (flight ID and other information), except for the altitude readout, just as if it were a normal flight. Our aircraft could probably be radar separated laterally by between 3 and 5 miles, depending on the phase of flight and a bunch of other factors. Vertical separation (altitude assignment) would be based on the other traffic's altitude readout and our own altitude as reported by our pilot.

The enroute radar systems at a regional Air Traffic Control Center would generally be able to track a primary return. However, at the end of the flight, the destination Approach controller might not have a system (such as ARTS IIIA - Radar Tracking & Beacon Level) that could track and predict primary returns. I guess this would probably mandate an increase to higher separation minima than usual, during the final phases.

I'm not an air traffic controller or anything, and I'm not going into excruciating detail on all the separation minima and equipment and procedures; there are books available; I think you have the idea now.

Onto Ellen's specific complaints ...

Reasons for being concerned about the lack of a working transponder are: an aircraft with invalid altitude data is not eligible for processing by the conflict alert function, and in order to enter a Terminal Control Area an aircraft must be equipped with a 4096 code transponder (so without a transponder the pilot could not fly into Newark, Kennedy, La Guardia, Atlanta, Dallas/Fort Worth, etc.). Agreed this is not an immediate major safety problem, but there are good reasons not to proceed without a transponder.

There are two issues here: Conflict Alert, and transponder requirements.

Conflict Alert is a set of features on some of the fancier Approach controller's radar systems. It is worth noting that only some of the radar systems have this feature (for example, ARTS II doesn't.)

The first kind of Conflict Alert has to do with the terrain/obstruction clearance map programmed into the system. Basically, when an aircraft is off the correct landing approach path, the system warns the controller.

The other Conflict Alert feature has to do with converging aircraft. In an IFR environment, this is just an additional safety feature; the separation criteria already provide for airplanes not be close to each other. It would warn the controller if the airplanes got closer than 3 miles. Of course, with arrivals effectively slowed down due to increased separation minima, the controller can simply monitor the separation manually.

For Conflict Alert to work, it has to have the plane's altitude readout from the transponder. So, if your transponder is not squawking your altitude, you would indeed lose these extra safety features. Lots of IFR flights are conducted to or from airports which don't have radar services available. Anyway, Conflict Alert is often turned off at ones that do.

Your statement about not being able to fly into a major airport (inside of a TCA) without a transponder is simply false, and appears to stem from an incomplete knowledge of the relavent regulations. Maybe you just heard someone briefly explain the rule in one sentence or something.

You can't fly into various kinds of airspace unless you have an operating transponder. In particular, you can't fly into the 30 nautical mile "Mode C Veil" around a TCA without an altitude encoding transponder. Unless the controllers authorize you to do so. To wit:

FAR 91.215 (d) ATC transponder and altitude reporting equipment and use; ATC authorized deviations. ATC may authorize deviations from paragraph (b) of this section -- (1) Immediately, to allow an aircraft with an inoperative transponder to continue to the airport of ultimate destination, including any intermediate stops, or to proceed to a place where suitable repairs can be made or both, (2) Immediately, for operations of aircraft with an operating transponder but without operating automatic pressure altitude reporting equipment having a Mode C capability; and (3) On a continuing basis, for operations of aircraft without a transponder, in which case the request for a deviation must be submitted to the ATC facility having jurisdiction over the airspace concerned at least one hour before the proposed operation.

If you refer to the Airman's Information Manual (170), or the Air Traffic Controller's Handbook (5-41), there are additional notes on the subject.

I don't understand the sources of some of the people making various claims about the air traffic system and its risks. I am just a simple four-month old private pilot (not even instrument qualified) and my information comes from my primary training, reading basic textbooks, and asking questions to the local FAA experts (the folks at Boston Center.) I wish people would research things more before making scary statements.

If people would like to continue this discussion in this kind of detail, I would be willing, but I consider this all to be a sidetrack from the essential points about the airliner story and how IFR flight works. Not to mention whether the Airbus is safe or not.

My messages on the subject may have been somewhat charged, and if I have needlessly offended anyone, I apologize. However, the misinformation and misconception of issues surrounding flying is generally enormous, and I felt compelled to introduce a few facts and context into the discussion. I hope anyone has found this useful.

There are definitely risks associated with aviation, but unfortunately it's a technical enough subject area that it can be difficult to understand and evaluate without alot of detailed knowledge.

I think that the risks associated with systems such as fly-by-wire (remember that?) is a useful topic for discussion here, especially in broad terms of raising the basic risk awareness. I would be wary of certain kinds of micro-analysis however, unless you're pretty sure of what you're talking about.

Have you ever noticed when you read a newspaper or watch television news, that, quite often, technical issues you happen to be familiar with are misunderstood and distorted? I hope that similar treatments of our varied issues will not become the usual practice in RISKS.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Martyn Thomas <mct@praxis.co.uk> Fri, 9 Nov 90 11:04:27 BST

Electronics Weekly (November 7 1990, front page) reports that there is a software fault in the payphones manufactured by Paytelco (a GPT subsidiary) and used in the UK by Mercury. They are "exported to >40 countries".

The software fault allegedly allows a phonecard holder to avoid paying for

calls. No technical knowledge or special equipment is required. EW reports that the faulty software has been rewritten, and that replacement ROMs are being installed in all payphones.

In the same issue, EW reports a different fraud involving restoring the holograms on used British telecom phone cards. EW claims to have seen the restoration demonstrated. They have not published details of the method, but hint that it involves "phase changes" in the polymers which store the holograms, through reducing the temperature of the card.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

***** plain paper faxes keep a copy of all received material

Jan Christiaan van Winkel <jc@atcmpe.atcmp.nl> Fri, 9 Nov 90 12:34:44 MET

I was asked to change the paper on out FAX machine today. I took a 'kit' we have for this purpose, and saw that I also had to change the 'toner-roll'. This is a roll of carbon paper (sort of) that actually prints the message on the (plain) paper.

I saw that all messages printed on the FAX, are also 'burned' in the carbon paper (well, that's how the thing works). This means that even if I stand next to the machine to receive a private message, people can later just open the FAX machine and read the message. Even worse, since people are not aware of this 'copy' on the toner roll, they just dispose of the roll in the garbage can.

I wonder how many people know about this 'feature' of plain paper FAX-es...

Jan Christiaan van Winkel Tel: +31 80 566880 jc@atcmp.nl AT Computing P.O. Box 1428 6501 BK Nijmegen The Netherlands

Customers limiting programmer access to their systems

The Programmer Guy <jkimble@bally.bally.com> Mon, 5 Nov 90 11:49:42 PST

Jerry Leichter writes:

> If the courts uphold Logisticon, it's certain that in the future

> companies will not be willing to allow access to their systems by their

> software suppliers. At best, they might allow access only from

> locations controlled by the company, so that they can quickly lock out> the supplier.

Given all the press on these types of events, many of my clients have enacted some new policies to protect themselves. Here's the most restrictive... (thanks, Logisticon):

Before I can dial-in to make a change to a casino's on-line computer, I nnhave to

draft a memo outlining my expected changes and file it with the casino's MIS department 48 hours in advance. After it's been reviewed and approved, the modem is turned (using human call-back verification of identity) and I am permitted to make my changes. Within 72 hours of logging in, I have to file another document with the Gaming Control Board outling everything that was done, files that were changed, why they were changed, dates, times, etc. On the east coast, this paperwork is filed with a division of the State Police so lies can cost you not only a civil suit, but criminal charges (perjury, etc.) as well.

Other steps my clients have done to protect themselves include requiring me to put the original source code tapes in a safety depositn box they can immediately access so that any problems I create -- intentional or accidental -- can be "fixed" by applying the virgin tapes.

As you can imagine, this extra bit of work greatly lowers programmer productivity, especially for the simple, one-line changes; instead of working to isolate and resolve problems, I spend a lot of time drafting memos and reports.

At least in this part of the gaming industry, basic programming jobs involve 70% code/theories/debugging, and at least 30% communications skills.

Jim Kimble,	jkimble@bally.bally.com
Consulting for Bally Gamir	ng uunet!bally!jkimble

[I doubt if that is a Bally High. PGN]

Student hackers arrested

Dave King <71270.450@compuserve.com> 06 Nov 90 22:46:48 EST

NEW YORK (UPI) -- Two Staten Island youths were arrested on charges of invading and disrupting the computerized voice mailbox system of a Massachusetts firm, costing the company \$2.4 million, officials said Tuesday [6 Nov 90]. State Police Senior Investigator Donald Delaney said [...] as a result of the hacker operation, the International Data Group of Framingham, Mass., lost scores of these messages. Delaney said an intensive two month investigation led police and U.S. Secret Service agents to Daniel Rosenbaum, 17, of 42 Caswell Ave., and to a 14-year-old associate, whose identity was not disclosed because of his age. He said exhaustive experimentation by the two suspects enabled their home computer to dial into the system and obtain the password to use it.

The youths then changed the passwords for various units in the system, which resulted in the loss of many important messages. "In addition, the company had to shut down the system for 18 days to revamp it," Delaney said. He added that the teenagers "made bomb threats and other harassing messages to the company, and when they were in contact with women employees, they made sexually explicit remarks to them." Delaney said Rosenbaum stated that he focused on the Massaachusetts firm "in anger" when it failed to send him a poster which was supposed to accompany a paid subscription for a computer game magazine

published by the company.

Both teenagers, students at Wagner High School, were charged with computer tampering, unauthorized use of a computer and aggravated harassment. [...] If Rosenbaum is convicted of the charges, he could be sentenced to four years in prison, Delaney stated.

Sprint's new calling card

<[anonymous]> Wed, 7 Nov 90

Jim Morton raises a couple of serious risks with respect to Sprint's new calling-card system. I used to work for the company which builds the hardware and software Sprint is using. At a major presentation the manager in charge of the project presented the voice-recognizing, Social-Security-number system. He presented his own card, prominently displaying his SSN, which I copied down.

During the presentation, he explained that Sprint wanted to use voice technology so that people wouldn't have to write down as many things (card number, password number). Their customer surveys also indicated that people found a 14-digit number "hard to memorize" and that a 9-digit number "which was one they used all the time" would be "more convenient."

After the presentation, I arranged to speak to the manager. I raised the same objections Jim Morton noted in his article. I also pointed out that he (the manager) had put his SSN up in front of close to 120 people and if any of them were of a mind to be nasty he could be in trouble. He scoffed at my concerns and assured me that Sprint's customer-survey managers were aware of the problems.

He also stated that he disbelieved anyone could "do any damage" simply by possessing another's SSN. I tried to explain, but he brushed me off and left. I spent the rest of the afternoon staring at the napkin on which I had written the manager's SSN. As I saw it, I had three options:

1.Do nothing.

- 2.Try to find someone else in the company hierarchy to listen to my complaints.
- 3.Construct an object lesson which would convince the manager of how real my objections might become.

I chose option 1. I had raised the objections as forcefully as I dared (the manager was several levels higher than I in the hierarchy, and *much* more senior). Trying to circumvent channels is discouraged in the extreme in this company. I already had a reputation as a serious maverick. I didn't have any evidence to support my objection; all I had was a set of vague assertions which, to me, seemed to be common sense. Pitted against the expressed desires of our customers (Sprint), you can guess how much weight this would have been given.

With respect to option 3, I can think of at least six ways to make someone's life seriously miserable if I have their SSN. I thought about using the manager's SSN for this example, but since most of the ways I know of involve committing misdemeanors or felonies, I decided it wasn't worth the risk. It also might harm his family who I felt did not deserve to suffer.

In hindsight, I could have bucked the chain of command anyway. But if put in that position again, I'm still not sure I would. In a way, I feel that people have the choice to use Sprint's stupid, vulnerable system. I know I won't. I also don't have a bank-by-phone system, nor do I have an answering machine that can be manipulated from a remote touchtone phone, nor do I give out my SSN to anyone who can't prove a need or legal requirement for it.

But then, maybe I'm a fossil in the information age.

Employer's use of credit reports

Jerry Leichter <leichter@lrw.com> Thu, 8 Nov 90 09:03:00 EDT

Use of Credit Reports In Hiring Draws a Caution

Managers who use credit reports to screen job seekers, beware: Spurned applicants have a right to know.

That message is going out from federal officials, who have grown concerned over that companies may be sidestepping the law governing the review of personal credit information. The law permits companies to consult credit reports when evaluating job seekers, a practice that has boomed of late among employers who see the reports as a way to judge the character of prospective workers. But the law also demands that applicants know when they've been rejected "wholly or partly" because of data in their credit file - a step that, critics have charged and officials fear, many employers ignore.

The [FTC] ... underscores the requirement in articles that two large purveyers of credit reports, TRW and Equifax, agreed to circulate ... to ... their customers. If they fail to comply with the disclosure requirement, the pieces note, employers may face suits from both the job applicant and the FTC.

The credit data agencies were "very pleased" to disseminate the warnings [according to the FTC].... One factor ... may be the prospect of new restrictions on their activities, now pending in Congress. ... TRW even changed its contracts to clarify the notification rule for employers.

There's actually more to this issue than the WSJ mentions. Business Week had an article on it a couple of weeks back. At one time, references were a fundamental part of the hiring process. Changes in the legal climate - particularly many successful lawsuits by former employees who felt they had received unfair recommendations that cost them jobs, plus increasing restrictions on what an employer may legally ask of a job-seeker - have caused many of the traditional sources of information to dry up. Recommendations these days are pretty uniformally bland and uninformative, and interviewers have gotten very, very cautious. So a recent trend is to use credit and other similar reports.

The problem is that the reports often contain data that is unverified or inaccurate - especially since there is a growing market for "el cheapo" reports for entry-level employees. Even when the reports are accurate, they may contain information that an employer is legally not permitted to have. Two specific examples that have cost people jobs (illegally, if they can prove it): Reports of arrests that did not lead to convictions, and reports about workman's compensation claims. (The view among some employers is that anyone who filed for workman's compensation is just out to milk the system, and they don't want the headache - Business Week has a quote from one employer saying exactly that, even more harshly than I just did. They also give an example of someone who was genuinely injured on the job, took his workman's compensation, recovered - and has been consistently turned down for jobs ever since.)

The reason that the big guys like TRW and Equifax are willing, even eager, to help out on issues like this is that the last thing they want is a lot of small low-ball competitors who not only steal market share from them, but also bring public (particularly, Congressional) attention to the business. While in this case their cooperation may be useful, it's well to remember that ALL of the credit companies have been involved in problems, even scandals, in the past; and that it's a classic pattern for regulated industries to come to like the umbrella of regulation they live under: It keeps competitors and critics out.

-- Jerry

✓ Computers lead to greater monopolization?

Jim Griffith <griffith@dweeb.fx.com> Wed, 7 Nov 90 09:40:00 PST

I heard a radio report saying that someone back east has filed a class action lawsuit against a number of airlines, charging them with violating anti-trust laws. The suit claims that the predominance of live-feed computer systems in the airlines industry lends itself towards a situation where airline companies can instantly find out what their competitors are charging and change their prices accordingly. A number of airlines were named in the suit.

I'd appreciate someone coming up with a newspaper article or something more definitive than what I'm reporting.

Jim

risks when computers replace humans (was: Expert System ... Loop)

Martyn Thomas <mct@praxis.co.uk> Mon, 5 Nov 90 16:51:47 BST

I wrote:

- > This report *explicitly* referred to an expert system. The point of my
- > original posting was that an expert system which provides advice, in
- > circumstances where a decision must be made and there is insufficient time
- > for the commander to analyse the situation him/herself, is effectively
- > making the decision. Many who followed up agreed with this viewpoint.

... and davis@ai.mit.edu (Randall Davis) replies:

: Fair enough.

:

:

:

: Note also that a small variation on your fundamental claim is equally true:

: ... an EXPERT who provides advice, in

- : circumstances where a decision must be made and there is insufficient time
- : for the commander to analyse the situation him/herself, is effectively

: making the decision.

: That is, as is frequently true in these situations, not only is this not a : matter of expert systems, the computer itself is almost competely irrelevant. :

: It's a matter of being in a complex, time-constrained situation and needing to : make a decision. If you don't have the time to consider carefully what to do, : you're just about equally up the creek whether you get the advice from a : machine or from another human being.

This is true, but there are characteristics of computer systems that make the risks different (and less acceptable) than the risks from humans in the same role.

This is the major reason for the RISKS Forum, so I don't need to list the characteristics here. They include the complexity of the systems, the difficulty of assuring that the system functions as intended, and the extra risks if the system is replicated many times, so that the same fault may appear in many places.

Randall Davis continues:

: The moral of the story: try not to put yourself into those positions in the : first place. Neither computers nor humans will get you out of it, and neither : of them is to blame for your predicament.

I agree. There is a danger that the expert system will be trusted to a greater extent than a human expert, and that this will lead to commanders being sent to places where they would not be sent if only human experts were available to help. It is important to remember that the expert system, like any computer system, is complex and probably contains errors. Add to this that it is effectively in the loop (in the circumstances of the original discussion) and we can have a sensible discussion about whether it is a good idea to deploy the system.

Finally, but very importantly, there is the question of who is accountable for the consequences of errors. In the case of the human expert, accountability is clear and liability may follow. If the accountability (and possible liability) is not clear for the situation which uses a computer system, then I believe that the system should not be used in a critical application. In my view, the organisation which puts the system into use should be liable for any injuries it causes, (and I would expect a prudent organisation to pass this liability to the company which developed the system, through the development contract).

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

Villanova University Computer Ethics course Group Project

<21202764@VUVAXCOM.BITNET> Wed, 7 Nov 90 20:35 EST

I represent a group of Computer Science majors at Villanova University, Villanova, PA who are currently doing a project in a Computer Ethics course. I am writing in response to a story posted in the RISKS forum on OCT 18 -`Flawed Computer Chip Sold For Years'(<u>RISKS digest 10.54</u>). Our group project is to analyze this case in terms of present day ethical theories and give a class presentation on it. Thus, we have a few questions about it:

- 1. I need more details/specifics on the chip.(i.e. what was its model number, what was its design flaw, etc).
- 2. Are there any other journals/newspapers where the story appeared?
- 3. What has National Semiconductor done since the article in the newspaper revealed the problem?

If anyone out there could send any other pertinent information about the case, we'd appreciate it. Replies may be sent to my bitnet address: 21202764@VUVAXCOM. (I do not know if I have a UUCP or CsNet address).

Jonathan Gacad (21202764@VUVAXCOM), Bob Durbin, Lisa Cofey, Al Giordano

"The Devouring Fungus" at a bookstore near you

Gene Spafford <spaf@cs.purdue.edu> 8 Nov 90 00:07:01 GMT

I just recently got a copy of "The Devouring Fungus: Tales of the Computer Age" by Karla Jennings (W. W. Norton & Co., ISBN 0-393-30732-8, \$10.95).

As can be gathered from the unusual title, this is not exactly a computer textbook. What it is, is a collection of anecdotes and stories about computer technology and the people who spend their time working with computers. The stories range from historical to modern-day, and most are amusing to read. Not all are firmly grounded in documented facts, but that doesn't detract from the amusement factor; even the apocryphal tales convey a sense of the attitudes and foibles of the "computer geeks" who have shaped our community. The tales related in the book read like a cross between items in the Risks digest and postings to the alt.folklore.computers newsgroup. Many of the stories will be familiar, but that is what makes them folklore -- we've all heard variants of these stories, and probably repeated a few in turn. This is the first time I have seen anyone collect so many of them together, and in such an amusing and readable way.

For \$11, this is a must buy if you're into computers. My copy is going in a place of honor next to my Hacker's Dictionary, and just down the shelf from my Sidney Harris cartoon book. Check it out yourself.

Gene Spafford NSF/Purdue/U of Florida SERC Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-2004 ...!{decwrl,gatech,ucbvax}!purdue!spaf

4th Annual Computer Virus & Security Conference

Gene Spafford <spaf@cs.purdue.edu> 6 Nov 90 19:36:34 GMT

> Call for Papers 4th Annual Computer Virus & Security Conference March 14 & 15, 1991 in New York City

Sponsored by the DPMA Financial Industries Chapter In Cooperation with ACM SIGSAC and The Computer Society of the IEEE

The 4th Annual Computer Virus and Security Conference will feature more than thirty speakers on the topics of computer viruses and "vandalware," computer law, and computer security. Approximately twenty are well-known experts in the field, and fifteen or more will be selected on the basis of submitted papers.

Held on Thursday and Friday (Ides of March) at the New York World Trade Center, this major event features:

* Identification of latest threats to SNA, DEC, PC, MAC, X.25 and UNIX.

* Tools and Techniques: What the major corporations are doing.

* Specific Countermeasures: From labs, other companies, commercial vendors.

The Conference traditionally covers recent outbreaks and experiments; virus/intruder prevention, detection and recovery; product demonstrations and ratings; and special attention to LAN, PBX, SNA, OSI, E-Mail, and legal issues.

This year's focus topics are as follows:

* Prevention, detection and recovery from viruses and other harmful computer programs.

- * Original research on these and related topics.
- * Recovery from the Wall Street Blackout and the Novell Virus.
- * Case studies of computer and network security.
- * Surveys of products and techniques available.
- * Computer crime and related actions.

The bound Proceedings will include both the accepted papers and also discursive articles by the invited speakers. There will be four concurrent conference tracks each day:

Thursday will feature the Main Track, Products Track, Research Papers, and a special Trap & Prosecute track geared to law enforcement and criminal justice personnel.

Friday will feature Main, Products, and Research tracks, and a How to Recover track strongly requested by returning attendees from last year.

In the past, this conference has been featured in BYTE, CIO, Communications (ACM), Computer (IEEE), Computerworld, Data Communications, Data Center Manager, Datamation, Info World, Macintosh News, MIS Week, Network World, and Unix Review. It is sponsored by the Data Processing Management Association Financial Industries Chapter in cooperation with ACM SIGSAC and the IEEE Computer Society.

Attendees may make use of discount airfares (43% off Continental) from anywhere to New York, including both adjoining weekends. The Penta Hotel (formerly Statler Hilton) has reserved a block of Conference rooms at \$89 per night. Conference itself includes luncheon and quarter-mile-high hospitality at Windows on the World Restaurant.

Target audience includes MIS Directors, Security Analysts, Software Engineers, Operations Managers, Academic Researchers, Technical Writers, Criminal Investigators, Hardware Manufacturers, and Lead Programmers. Registration (202-371-1013) costs \$275 for one day, \$375 for both, with a \$25 discount for members of cooperating organizations (DPMA< ACM, IEEE-CS).

Submissions to the conference may be either as an extended abstract or a draft final paper. Four copies of each submission should be *received* by the program chair no later than Tuesday, January 8, 1991. Each submission must contain a brief abstract (approx. 200 words), and a header identifying the names, affiliation, address, and e-mail address (optional) of all authors. Successful submitters or co-authors are expected to present in person. Decisions will be announceed by Feb. 12, 1991.

Submissions are invited on all aspects of the conference, and particularly on new research in the area of vandalware and countermeasures.

Program Committee: Richard Lefkon David M. Chess Stephen R. White NYU, DPMA IBM IBM Thomas Duff Frederick B. Cohen Gene Spafford AT&T Bell Labs **Purdue University** ASP Research Dennis D. Steinauer Gail M. Thackery Kenneth R. van Wyk NIST AZ Attorney General's DARPA/CERT Office 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 I 🔶 🕨 🕤 🖉 🗤 🚀 Search RISKS using swish-e Report problems with the web pages to the maintainer



<bahn_pr%ncsd.dnet@gte.com> Fri, 9 Nov 90 16:04:31 -0500

The Washington Post, New York Times and USA Today had ordered national vote trend analyses from Voter Research and Surveys, a company set up to do exit poll surveys and have the results analyzed by 3:30pm on Election Day, 6 Nov 90. A computer glitch prevented the results from being available at all on that day. VRS had the data, but the weighting program did not work. [Abstracted by PGN from `Computer Mishap Forces shift in election coverage, Major Newspapers

faced with delays in polling data', by Lynn Duke, staff writer Washington Post, 7 Nov 90]

Now what i found interesting was the idea of Sam Donaldson screaming into some programmers ear while a camera is pointed on him. "Fix the program or we'll do a story on you buddy." :-)

There are some interesting risks. First that unclean data was used and second that the big news agencies now all use the same polling source. What a risk if someone hacked them to create false trends. [bahn_pr]

✓ Voting electronically from home (revisited)

John Roe <johnr@hpltbg.fc.hp.com> Mon, 12 Nov 90 13:27:39 MST

A Boulder CO group has rediscovered Bucky Fuller's 50-year-old suggestion that everyone should be able to vote telephonically from home or wherever.

"The system is based on a personal computer hooked into [the] telephone line. [Local activist Evan Ravitz] also loaded a list of registered Boulder County voters into the computer's memory, and the system checks names against a six-digit code based on date of birth. Callers enter their selections for the ballot by entering numbers on a Touch-Tone telephone. [...]

"Boulder County Clerk and Recorder Charlotte Houston ... placed a call to the system on Monday and found that could could have voted for her son and daughter by providing their birth dates or Social Security numbers."

[Abstracted by PGN from `Phone voting? Boulder group says it's time', an AP story from the Loveland, Colorado, Reporter-Herald, 6 Nov 1990.]

I found this article alarming for a number of reasons:

First, the possibilities for massive fraud are probably obvious to all RISKs readers. For example, if (as implied by the article) one can vote for another by simply knowing either the birth date or their Social Security number, with the hardware already in my own basement plus an appropriate database (which shouldn't be too hard to come by) I could have easily changed the outcome of a number of races and constitutional amendments here in Colorado during the November 6th election. With a concerted effort I could have chosen any candidate I wished. If I knew which registered voters had not voted recently, I could even make a reasonable effort at making my fraud somewhat less detectable.

Second, I was disturbed (but not surprised) that the article emphasized the "gee-wiz" aspect of the idea, but mentioned the RISKs only in passing, and ended with a statement that implied that concern over fraud were irrelevant and paranoid. The token assurances of Mr. Pelton only serve to support this perception. I have come to expect that the popular press is ill-equipped to understand, evaluate, and explain the risks of technology to their readers (or viewers, in the case of television). This latest example only reinforces my

expectations.

Finally, and perhaps most significant, was the cavalier attitude of Mr. Ravitz toward the possibility of fraud, and his obvious lack of understanding of the problem. The current system is NOT based on honesty: it is based on physical security. If it is sufficiently hard for the same person to vote multiple times, voter fraud can be reduced to acceptable levels (but not eliminated, of course).

In my precinct, I could conceivably vote two or three times before the election officials would start getting suspicious. If I spent the entire day driving around to various polling places in northern Colorado, I could perhaps vote a few dozen times. But to influence the outcome of the election would require a large number of cohorts; a task I could accomplish by myself from the comfort of my own home if Mr. Ravitz's proposal becomes law.

I wonder if we would be permitted to vote on changing Colorado's election laws to permit voting by phone, by voting by phone? The outcome of such a vote could be enlightening ...

John Roe, Hewlett-Packard, Colorado Integrated Circuits Division, 3404 EastHarmony Road, Fort Collins, Colorado 80525-9599(303) 229-4554

Marclays' security: apologies!

Pete Mellor <pm@cs.city.ac.uk> Tue, 13 Nov 90 11:30:57 PST

In <u>RISKS-10.50</u>, in an item entitled "Hackers blackmail five banks (UK)", I gave excerpts from a newspaper report about the breach. I followed this with an anecdote told by the manager of the local branch of a chain of off-licences, who found that, after sending in his completed order to the main warehouse, what appeared to be credit card transactions from Barclays' Bank were displayed on his screen.

Shortly thereafter, I received a phone call from the head of Information Security at Barclays, who was puzzled by the incident, and requested further information. Barclays' investigation revealed that the credit card transactions were in fact records of purchases made using the particular card at that off-licence, and others of the chain in the area. There was therefore no breach of security, since, of course, the manager had the right of access to that information. The incident was *not*, as I first thought, due to unencrypted transactions being transmitted over the public telephone lines being received by the wrong terminal. The only problem appears to have been a minor glitch which caused a file of credit transactions on the local machine to be displayed when my friend was not expecting it.

So apologies to Barclays Bank!

I hope that Barclays' security department are happy to let me set the record straight via RISKS, which they obviously monitor, and perhaps they would care to add some comments of their own.

Moral: Check your facts before passing on anecdotes which you hear in pubs!

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

🗡 Juicy 911 RISKS

Steve Smaha &maha@DOCKMASTER.NCSC.MIL> Sun, 11 Nov 90 13:51 EST

"911 calls are ripe for trouble" 11 Nov 90 Austin American-Statesman, BLACKSBURG, VA (AP)

These are hardly salad days for Montgomery county law officials. Last week, police were testing the county's 911 system, scheduled to begin operating next month, when the dispatcher received 10 calls that were traced to the home of Linda and Danny Hurst. She tried to call the line, but it was busy. When she hung up, she received another call from the same line. And another.

Deputy sheriff tracked down Linda Hurst. "I told them I'd locked my house and there shouldn't be anyone in there," she said. Police, concerned that someone had broken in, asked Hurst to meet them at her house. She parked in front of the house, and walked up to the front door. "But they said, 'Ma'am, step back please.' I looked back and they had their guns drawn. They were serious," Linda Hurst said. "They went through the house, but they couldn't find anybody, so I went inside."

Finally, Linda Hurst's brother spotted the culprit - an overripe tomato. The tomato was hanging over the telephone in a wire basket, dripping juice into the couple's answering machine.

Chief Deputy Milton Graham said the tomato juice apparently got into the telephone's dialing system and caused it to dial the sheriff's office. "We're not sure how. Maybe they had speed dialing and it shorted out," he said. "I didn't know the answering machine could even dial out," Linda Hurst said. "It's just supposed to take messages."

Ke: UK Software Engineer Certification

Brian Tompsett <bct@cs.hull.ac.uk> Mon, 12 Nov 90 12:24:00 GMT

This note supplies greater detail about the steps involved in the certification of Software Engineers in the UK. It is in response to several inquiries requesting more detail after my last contribution to RISKS (Sept 21, 1990).

In answering the questions let me point out that the UK does not have Software Engineering *specific* certification. Nor does it have *certification* in the strict sense that is being discussed in the US at present. When I have detailed the routes available in the UK you can decide for yourself how this relates to what does/will exist in the US.

Let me start by describing the qualification route from High School through the maze of qualifications and certifications. I can deal with how existing Engineers fit into the picture later.

.----- Government ------. Charters | Approves Curriculum Body v High School T | University Engineering | Entrance Council | Exams | Accredits I Society v University <-----Accredits Degree Course--- Professional Society L | Accredited | Engineering .----' | Join Society | Degree 1 v L Student member Graduate Employment <--Approves training-----' | Get experience | Certified | Engineering | training and experience ٧ **Corporate Member** Chartered Engineer-----Ι Status 1 | More | Experience | Outstanding | Achievement I v v Fellowship of Society Fellowship European of Engineering Engineer

The route illustrated in the above diagram is not specific to Software Engineers, but is the generic model for all Engineers in the UK. The student starts by taking a degree course at a University; this may be a B.Eng, M.Eng or B.Sc. degree. In order for this degree to be considered a suitable education for an Engineer the course must be accredited by the appropriate professional body. The accreditation examines the curriculum, the facilities, the teaching department and the institution itself. After graduating the student is expected to take a position that will provide practical engineering training and real experience. The training and experience is logged in the graduates own engineers logbook and signed-off by qualified engineers and trainers. The professional society provides the employer with the basic structure for this. When the Graduate Engineer has gained sufficient experience (minimum 4 years) he may apply to be a Chartered Engineer. Admission to Chartered Engineer can only be made through a professional society and normally corporate membership of the society requires the same entry qualifications as Chartered Engineership. On joining the society the member is required to follow professional code of conduct and code of practice. The admission procedure involves vetting the applicants qualifications, receiving references from the applicant's sponsors who are normally two other professional members and an interview.

The Professional Society itself is accredited by the Engineering Council. The accreditation examines the Societies methods and procedures for admission, course accreditation and so on. The Engineering Council needs to ensure that Engineers from all the different disciplines are equally qualified to be Chartered Engineers. The area represented by the Society must also be one that is considered as Engineering. This was a major hurdle for the British Computer Society to show that "Information Systems Engineering" is Engineering and qualified practitioners are worthy to be Chartered Engineers. This process took four years.

The Pan-European Engineering element should also be noted. Someone qualified as a Chartered Engineer may also apply for the title "European Engineer". This is a title that is recognised across Europe. It also has its own code of conduct in addition to the one applied by the professional society. A fully qualified Software Engineer in the UK would therefore be attributed as:

Eur.Ing John Doe B.Sc, C.Eng, MBCS (or similar.)

Others may qualify as Chartered Engineers who do not follow the above route. They may have become Software Engineers before the terms Computer Science or Software Engineering existed, or have switched disciplines and previously qualified in something else. They may have no formal qualifications at all and have come into the profession through experience alone or they may have overseas qualifications and experience. These groups of people are admitted after having their qualifications and experience verified in a similar manner to other applicants. Their education and training is compared to the standard curricula. This sometimes involves examination of the students class transcripts and the details of the course syllabus. In the absence of a contemporaneous experience and training record a detailed Curriculum Vitae needs to be validated. This usually involves finding other Engineers who can act as referees and certify that the actual work experience claimed actually took place and was of sufficient quality. This is usually done by initialing copies of the curriculum vitae item by item.

Just to confuse the issue, the UK has a Software Engineering Examination Board who issue certificates of competence in Software Engineering. These are not related to the kind of Software Engineer certification we have been discussing. The SEAB is involved in the training of people in the SSADM method that has been mandated for use on UK Government work.

Brian Tompsett, Computer Science, Hull University.

Software Protection Tool

"DAVE ERSTAD" <derstad@cim-vax.honeywell.com>

9 Nov 90 17:06:00 CST

In the October 18th issue of Electronic Design News there's a blurb about a new product which obfuscates source code by changing variable names, removing comments, etc. The intent is to allow software to be distributed in source form while still protecting proprietary knowledge.

The RISKy part is what some people believe (either the company or the reviewer, I'm not sure which). The last statement in the article is

"Distribution also ensure that the producer receives virus-free code, because VIRUSES CANNOT OPERATE IN SOURCE CODE" (emphasis added).

Dave Erstad, Honeywell SSEC DERSTAD@cim-vax.honeywell.com

complaints about Sprint's voice-card system

Steve Elias <eli@PWS.BULL.COM> Sat, 10 Nov 90 14:17:36 -0500

These complaints about Sprint's voice-card system are a bit silly! Where do yall get the idea that Sprint insists that one use their SSN as their ID number? A friend at US Sprint confirms that their internal literature makes no mention of forcing people to use their SSN.

Until you get some evidence that Sprint will not allow people to use numbers other than their SSN, please refrain from flaming!

/eli

Sprint's New Calling Card

Jerry Glomph Black <black@ll-null.ll.mit.edu> Fri, 9 Nov 90 16:49:14 EST

Obviously using the Social Security number as the basis of your FONCARD security number is pretty dumb. However, WHO tells Sprint this number? Presumably YOU, the customer. So, just feed them a number sequence which has high mnemonic value for you. Like maybe your phone number, or a slightly modified version of same. I've memorized my 14-digit `random' FONCARD number, but I use it a lot. Sometimes it's annoying to dial 11 digits of access code(1-800-877-8000), then the 11 digits of the destination number, then the bloody 14-digit number. My wife refuses to do this, so we got an AT&T card, where all you have to remember is FOUR DIGITS (tacked on to your 10-digit home number, which you presumably know). Anybody know why Sprint didn't just adopt this method? Chauvinism?

Even the police-state People's Republic of Massachusetts allows you to specify a bogus SS No. for your driver's license, instead of your real one, so long as your bogus no. doesn't duplicate somebody else's license no. I recently took out a Hawaii driver's license, and they DEMANDED (over my vociferous objection) the SS No. or else! I'm not mega-paranoid, so I complied. Any Federal privacy laws involved here?

Jerry Glomph Black, black@MICRO.LL.MIT.EDU

Ke: Carbons (<u>RISKS-10.59</u>)

Douglas W. Jones,201H MLH,3193350740,3193382879 <jones@pyrite.cs.uiowa.edu> 9 Nov 90 21:31:15 GMT

> I saw that all messages printed on the FAX, are also 'burned' in the carbon
> paper ... This means that even if I stand next to the machine to receive
> a private message, people can later just open the FAX machine and read the
> message.

This is not a new risk! For years, typewriters that use a carbon film ribbon have recorded every word typed on their ribbon. All you have to do to find out what was typed on a typewriter is to take out the ribbon cartridge, pull out the used ribbon and read it. The more errors and corrections made during tye typing, the more garbled the ribbon will be. The risk is at least as old as the IBM Selectric typewriter, and is well-enough known that it has appeared in many cheap detective stories.

Doug Jones

Your Flood Stories Please.

"Lindsay F. Marshall" &indsay.Marshall@newcastle.ac.uk> Mon, 12 Nov 90 16:16:05 GMT

Can anyone who has suffered a problem at their installation caused by water in *any* form (or in fact any other liquids....) or who has heard of such events please send me a summary of your experience. Information will of course be treated in confidence if you should so desire.

Lindsay

MAIL : Lindsay.Marshall@newcastle.ac.uk (UUCP: s/\(.*\)/...!ukc!\1/) POST : Computing Laboratory, The University, Newcastle upon Tyne, UK NE1 7RU VOICE: +44-91-222-8267 FAX: +44-91-222-8232

Ke: Corrected version of Virus Conf announcement (Re: <u>RISKS-10.59</u>)

Gene Spafford <spaf@cs.purdue.edu> Fri, 09 Nov 90 21:04:16 EST

The following address was missing from the announcement of the 4th Annual Computer Virus & Security Conference, in <u>RISKS-10.59</u>:

Dr. Richard Lefkon Virus Conference Program Chair 609 West 114th Street
New York, NY 10025 (212) 663-2315 Search RISKS using swish-e Report problems with the web pages to <u>the maintainer</u>



Wed, 14 Nov 90 09:19:28 EDT

The Wall Street Journal this week had two articles on privacy and technology that I thought RISKS readers might find of interest.

On Monday (13-Nov; page A-1) it reports on some new technologies that are

becoming available to the police. Two are of particular note: Pilotless surveillance drones developed for the military have been suggested as "just the thing" for the police. These are small planes - in techno-speak, they are UAV's (Unmanned Aerial Vehicles) - that can stay at 500 feet for about an hour. Currently, they carry cameras with telephoto lenses and infrared sensors; it's proposed that they could also carry chemical sensors to detect various chemicals used in drug manufacturing. None have apparently been used so far they are expensive (anywhere from \$20,000 to several million a piece) and the FAA has yet to approve their use.

And for those of you who think that calling from a pay phone is a way to avoid wiretaps - think again: The "roving bug" can find you. This is a device that does pattern matching on phone calls, looking for a particular voice. At least one successful prosecution has already been based on evidence obtained by such a device. The details aren't clear from the article, but apparently some 15,000 calls were intercepted, more that 5,300 from one person's office and some 450 from various pay phones. Just what the technology can do today isn't clear, but it is clear that very broad-scale monitoring of digitized conversations, with scanning for voices of interest, is possible if expensive today and will rapidly become cheaper and easier. Apparently such wiretaps were authorized by Congress in 1986.

The article also mentions other devices, like tiny pinhole TV cameras - one was installed over the urinals at a police station to find a vandal who was clogging the urinals, causing water to drip down into the chief's office. (Isn't it great to know what our tax dollars are paying for?) Also, LoJack-like devices are becoming much more widespread. (LoJack is a transmitter installed in your car. If your car is stolen, you tell the police; they turn it on and can track the car.) Smaller scale versions for protecting valuables exist, and systems that use satellites to allow tracking literally around the world are in the works.

On Tuesday (14-Nov; page B1) the Journal reports on the controversy surrounding a product soon to be introduced by Lotus. Lotus Marketplace consists of a CD containing information on some 80,000,000 households, including names, addresses, shopping habits, likely income levels, and even a catagorization (by Equifax) into one of 50 catagories like "accumulated wealth", "mobile home families", "cautious young couples", and "inner-city singles". Also included is a program - apparently at least partly a Hypercard stack - that provides an interface to the system. The whole thing costs \$695 for the program and an initial 5000 names; each additional 5000 names cost \$400. How Lotus keeps you from using the other information on the CD is unclear - presumably, you sign a license and they come after you if you breach the terms.

The program Lotus provides does not allow you to look up a particular individual by name, but of course if you know anything about him you can come up with a query that will find him and few others - and of course the unethical will hardly be stopped from developing their own search programs by the terms of a license agreement.

All of this information has been available for some time from mailing-list vendors. However, it's been expensive and "transient". What Lotus does is provide the information permanently and cheaply. Lotus says that to prevent abuse, they will not include telephone numbers (of course, CD's with telephone

number listings are increasingly available) and will sell only to "legitimate businesses" at verified addresses checked against a "fraud file". The license terms will limit the uses to which the data can be put and provide penalties for abuses. It astonishes me that anyone can imagine they can control how a small piece of plastic, indistinguishable from hundreds of like copies, will be used once it gets out into the world.

The debate, as presented by the Journal, is on familiar grounds. Anti: This is a major invasion of privacy - "They've crossed the line" (Marc Rotenberg, CPSR). Pro: There's nothing new here; Lotus is just making a service available to smaller businesses who couldn't afford it previously. "What this lets you do is send a few more pieces of mail. What's the harm in that? Lots of people like to get mail." (Dan Schimmel, developer of the system.) You CAN keep your name off the CD by written request to Lotus, Equifax, or the Direct Marketing Associations mail preference service. (It's an interesting question whether this actually keeps your name off the CD or just marks it as "doesn't wish to receive mail". While such a marking would keep legitimate users away from you, it would do nothing to stop abusers, like those the Journal suggests could look for "unmarried wealthy women over 65 in this neighborhood".)

The article contains a wonderful cartoon by Mark Stamaty. The scene: Two women, one (A) looking at and later opening an envelope. Prelude: "Every purchase gets recorded in psycho-data central. They'll have samples of everyone's handwriting. Soon millions of computer-driven autopens will transcribe junk mail in the handwriting of each person's best friend, spouse or lover."

- A) I got a letter from *Bill*!
- B) Maybe he wants to get back together.
- A) Think so?
- B) So what's he got to say? Is he sorry? Does he want to try again?
- A) He says I'm very special to him and to show me *how* special... he's offering me 40% off the newstand rate on a subscription to
 - Sports Illiterated!

-- Jerry

[With Dreamy Indolence, Lotus Leaves nothing to be desired? PGN]

Privacy concerns about new Lotus "Marketplace" product

Jeff E. Nelson <jnelson@tle.enet.dec.com> Wed, 14 Nov 90 09:53:47 PST

The following is extracted from an unofficial electronic newspaper edited and published within Digital for Digital employees. Reproduced with permission. The issues raised herein should be familiar to regular RISKS readers.

Jeff E. Nelson | Digital Equipment Corporation, Nashua, NH, USA jnelson@tle.enet.dec.com | Affiliation given for identification purposes only

VNS COMPUTER NEWS:

===============================

[Tracy Talcott, VNS Computer Desk] [Nashua, NH, USA]

Lotus - New program spurs fears privacy could be undermined {The Wall Street Journal, 13-Nov-90, p. B1}

Privacy advocates are raising the alarm about a new Lotus product that lists names, addresses, shopping habits and likely income levels for some 80 million U.S. households. Due for release early next year, Lotus Marketplace packs the data on palm-sized compact disks aimed at small and mid-sized businesses that want to do inexpensive, targeted direct-mail marketing. But critics say the product is just too good. "It's going to change the whole ball game," says Mary Culnan, an associate professor at Georgetown University's School of Business Administration. "This is a big step toward people completely losing control of how, and by whom, personal information is used." Janlori Goldman, a staff attorney with the American Civil Liberties Union, adds that the product raises "serious legal and ethical questions." Lotus' critics concede that the product offers little more than is already available from established mailing-list brokers. But they say it is a greater potential threat to personal privacy because of its low cost, ease of use and lack of effective safeguards over who ultimately has access to it and why. They also say that the way it is designed allows users to ask a series of increasingly specific questions about small subgroups of people - identifying, for example, unmarried, wealthy women over 65 in a neighborhood. "They've crossed the line," says Marc Rotenberg, Washington director for the nonprofit Computer Professionals for Social Responsibility. "It simply shouldn't be allowed on the market." Lotus counters that the product, still under development, has been tailored to address privacy concerns. No phone numbers will be included, it won't be available in retail stores and it will be sold only to "legitimate businesses" at verified addresses checked against a "fraud file," Lotus says. A contract will specifically limit its use and provide penalties for abuses. Owners will be be allowed unlimited use of the names and addresses they buy, at a cost of \$695 initially for the program plus 5,000 names and \$400 for each additional 5,000 names.

Permission to copy material from this VNS is granted (per DIGITAL PP&P) provided that the message header for the issue and credit lines for the VNS correspondent and original source are retained in the copy.

all US consumers on CD-ROM

Rick Noah Zucker <noah@cs.washington.edu> Thu, 15 Nov 90 09:47:13 -0800

This was forwarded to me: [Discussion of PBS item on Lotus deleted. PGN]

The database does not contain any of the data covered by the fair credit practices act so Lotus is under no legal obligation to let you see what they

are saying about you (unless you buy the product, of course...) and has no provision for allowing you to change what is in there.

The Lotus spokesman said that if people wrote a letter to Lotus saying they did not want to be in the database, they would be excluded. Unfortunately, the interviewer did not say to whom the letter should be addressed.

🗡 Kuwaiti citizen database

Jonathan Leech <leech@cs.unc.edu> Thu, 15 Nov 90 10:27:54 -0500

Last night's (11/14) BBC News reported that a computer database containing fingerprints and other information on all Kuwaiti citizens had been smuggled out of the country. Apparently the Iraqi government is attempting to eliminate all evidence of the nation's existence, and this database may be important in setting things up again (assuming the Iraqis leave).

Perhaps this may be considered an anti-RISK of government databases?

✓ Gas pump inaccuracies?

Paul Schmidt <prs@titan.eng.ileaf.com> Mon, 12 Nov 90 13:57:11 PST

I have noticed an interesting characteristic that seems to be shared by all self-serve gas pumps. They all shut off automatically _shortly_after_ reaching the amount I gave the attendant, but before reaching the next higher penny. (The gallons display continues to advance.) So what algorithm is used to determine the shut-off point? The fairest algorithm ought to be:

WHILE delivered_amount <= amount_wanted DO pump_gas

But I seem to be getting \$0.005 - \$0.01 more gas every time, because the pump seems to be doing:

WHILE delivered_amount <= amount_wanted DO pump_gas

Whereas if the gas company wanted to make an average of onehalf cent per transaction:

WHILE delivered_amount < amount_wanted+0.01 DO pump_gas

Is the public the group beneficiary of about \$0.005 per transaction due to what would otherwise be a bad algorithm? Did the programmer do this on purpose because s/he felt Big Oil wasn't paying enough? What implication might this have on computer controlled delivery of other liquids (insulin?) or gasses (oxygen?)

Paul Schmidt

prs@ileaf.com

"It's the computer's fault"

Andrew Klossner <andrew@frip.wv.tek.com> Wed, 14 Nov 90 14:20:38 PST

My wife and I visited a restaurant in Cannon Beach, Oregon for Sunday breakfast. The service was slow, but that's okay, we were sitting down and had coffee and plenty to read.

A distraught-looking hostess crossed the room to our table and asked me "Are you a computer expert?" "Why, yes," I responded. "Would you please come fix our computer?" As we walked to the back room, she cackled "Try to tell me I'm not psychic ..."

The "computer" turned out to be an electronic cash register, whose printer ribbon had slipped out of the feed mechanism. I fixed it and returned to my table.

Service continued to be very slow -- the family next to us left after waiting 45 minutes. To one and all, the hostess proclaimed "We had a computer problem, but it's fixed now and you'll get your food soon."

But the cash register was used only to print bills when the meal was over, and had nothing to do with slow food service, which apparently was caused by an AWOL server.

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

Ke: Voting electronically from home (revisited)

Li Gong <li@diomedes.UUCP> Thu, 15 Nov 90 11:58:24 EST

John Roe (in <u>RISKS DIGEST 10.60</u>) quoted a report that "A Boulder CO group has rediscovered Bucky Fuller's 50-year-old suggestion that everyone should be able to vote telephonically from home or wherever." and raised a few risks in the proposed scheme. He also pointed out that "The current system is NOT based on honesty: it is based on physical security. If it is sufficiently hard for the same person to vote multiple times, voter fraud can be reduced to acceptable levels (but not eliminated, of course)."

I would like to add that the current system not only provides physical security of identification, but also physical security against harassment. Nobody else is allowed to go into the booth when a voter, say Alice, is voting inside. On the one hand, this gives Alice privacy; on the other, she can vote according to her own will. Moreover, since this individual vote is among maybe a billion other votes, no ordinary person could find out for whom Alice has voted. This potentially discourage "buying" votes with money or menace, because it is difficult (if not impossible) to "physically" influence a voter at voting time and/or to verify a voter's vote afterwards. In any trivial scheme such as voting with SSN over a phone line, all these good features disappear. Professor David Wheeler (my PhD thesis supervisor at Cambridge) and I once worked on a voting scheme that supports these features and also allows voting by phone or post. This effort, together with a generalization of the idea into a notion of "zero-knowledge transactions", is still in progress (I hope :-).

Li Gong, ORA Corporation, Ithaca, New York (607) 277-2020

Voting by phone risks in error

Frank Hage <fhage@sherlock.rap.ucar.EDU> Thu, 15 Nov 90 14:34:49 MST

The risks assumed by John Roe in his note regarding the Boulder, Colorado demonstration of voting by phone are not valid. The system was *not* part of the official voting process, but was intended only to introduce people to the possibility of voting by phone. This fact was clearly mentioned in the articles the local paper (Boulder Daily Camera) printed and, in addition, the demonstration ran for three days prior to, but not on election day. It was emphasized that the votes cast using the phone based system would not be "real" and that voters would still have to go to the polls to cast legal votes. The organizers of the demonstration specifically mentioned that *if* this were an official voting method, a more secure authentication system would be necessary. They suggested that a security system similar to the one currently used for automated teller bank cards might be used. Each voter would receive a personal authentication number when registering, which would have to be entered correctly before the phone vote would be counted. Several other possible authentication methods were also mentioned, including "voice prints". Because this was only a demonstration, and would have no affect on the official vote count, they used the birth date of the voter, which they obtained from public voter registration records, as an example of the concept of requiring voter authentication.

One can easily envision mechanisms where the caller ID feature that many areas now have in place, could be used to foil attempts by people to cast large numbers of votes from one phone, even if the authentication system were compromised. As I see it, the risk of phone voter ballot stuffing is much smaller than the risk phone the voter's ballot would not be secret.

The only risks the demonstration illuminated was the risk of people making poor judgements about computer technology based on information provided to them by the popular media.

-Frank Hage (fhage@rap.ucar.edu)

Ke: Voting electronically from home (revisited)

Dan Sandin <sandin@uicbert.eecs.uic.edu>

Thu, 15 Nov 90 22:38:55 GMT

Although the potential risks of voting by telephone seem great, I think the potential benefit would far outweigh them.

For example, in the most recent election, I found myself rushing to the polling place near my home (since you can only vote at the registered polling place) and arrived too late. If I could have voted at a location near my work, or by telephone, problem solved.

So, how do we deal with the identification of voters by phone?

How does this sound: before each election, each voter is mailed a confirmation of registration (since, I believe, to vote one must be registered, and to register, one must have a permanent address) In this confirmation of registration would be a random number, with perhaps a checksum or something to discourage forgery, issued on a double blind basis. The user would have to punch in the registration number, with perhaps a ss#, birthdate, or other identification. However, leaving this out would encourange secrecy of voting.

For those who cannot handle vote-by-phone, of course, the old system would be available.

The problems of voter security seem easier than, say, credit card security. Unlike a credit card, "stealing" a single vote would not be worth much. This system would also permit simple absentee ballotting...

stephan meyers c/o sandin@uicbert.eecs.uic.edu

Ke: Computer Mishap Forces shift in Election Coverage (<u>RISKS-10.60</u>)

<tep@tots.logicon.com> Thu, 15 Nov 90 12:58:43 PST

>There are some interesting risks. First that unclean data was used and >second that the big news agencies now all use the same polling source. What >a risk if someone hacked them to create false trends. [bahn_pr]

All of the major news agencies have been using the same information base for at least 6 years now. It is called the National Election Service (NES), and its information is by definition "unclean" and "hacked to create false trends".

The NES reports any and all information from the official polling sources, but filters out all references to any candidates other than the Republicans and Democrats. This filtered (incorrect, incomplete) information is then made available to all of the news agencies. This filtering is, of course, done by computers.

There is a rumor that this intentional bias uncovered an interesting bug/assumption in some display software at one of the southern TV stations: The

display SW "knew" that there would only be info on two candidates, so it calculated the percentage information for the "second" candidate by subtracting the poercentage infomation for the first candidate from 100%. Unfortunately for the station, the local Libertarian candidate recieved enough votes (at some point in the voting), that the second candidate was shown to be in the lead (based on his votes + the votes for the Liberatrian).

Tom Perrine (tep) Logicon Tactical and Training Systems Division San Diego CA UUCP: sun!suntan!tots!tep +1 619 455 1330

✓ Election coverage software

&ary_Cattarin@dg_support.ceo.dg.com> Thu, 15 Nov 90 14:07:24 est

CEO summary:

Computerized and centralized election coverage poses a bigger risk than the "unclean data" and program glitches pointed out in <u>RISKS 10.60</u>. And this one is unfortunately intentional. The News Election Service, the central clearing house for election information, has their systems set up to deliver vote percentages that show the major party candidates' votes adding up to 100%, even when the major party candidates don't capture 100% (as they usually don't). . In the 1988 presidential election, the public was told that anyone who didn't vote for George Bush (shudder) voted for Mike Dukakis (bigger shudder). In other words, George + Mike = 100%. That was a lie; in fact George + Mike = about 99%. Small, but significant difference. Same thing happened here in Massachusetts last week: the third candidate took 2%, but most reports read "Weld 51%, Silber 49%" (not sure of exact numbers). Now, they can omit small guys if they want, but don't lie to the public as if they didn't exist. The point here is that a bad policy decision is multiplied by the technology used to spread lies and mistruths to the general public.

Ke: Juicy 911 RISKS (Smaha, <u>RISKS-10.60</u>)

Amos Shapir <amos@taux01.nsc.com> 15 Nov 90 12:50:03 GMT

This points out another class of risks: hidden features. I wouldn't be surprised if that answering machine contained the full circuitry of a phone, with the dial-out part disconnected; it is often cheaper to design a machine around an existing product than to redesign new down-graded part.

Likewise, a "dumb" answering machine may turn out to have undocumented remote-command capability, a computer terminal may have hidden escape code functions, etc. The obvious risk is that people who know about such features, might use more sophisticated methods than pure tomato juice to make the devices behave in ways their owners never anticipated nor took precautions too avoid.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, IsraelTel. +972 52 522255 fax: +972-52-558322amos@nsc.nsc.com

🗡 Ada Remarks

Paul Murdock <murdock@cvax.psi.ch> 13 Nov 90 10:48 +0100

In response to Chet Laughlin's note about ADA multitasking (10.50) ...

>The first lab involved two tasks running in parrellel. In reality it was >figured that the tasks would time-slice on a single machine. However, this was >not the case. The compiler would simply run the highest priority task until it >ended, and then run the lower task.

My understanding would be that, providing the highest priority task was always computable (and what is meant by time-slicing here is not exactly clear), then this behaviour is a valid interpretation of the text of the Ada standard :-

"If two tasks with different priorities are both eligible for execution and could sensibly be executed using the same physical processors and the same other processing resources, then it cannot be the case that the task with the lower priority is executing while the task with the higher priority is not."

[Par. 9.8:4, VAX Ada Ref Manual

("Digital-supplemented text of ANSI/MIL-STD-1815A-1983")]

... and note that my remark comments on the interpretation of the text and not the text itself.

Chet continues ...

>It was interesting to note that programs that ran correctly on SUNS did not >run correctly on the PS/2s - even though they compiled without change.

One of the most painful characteristics of the Ada standard is that although "its purpose is to promote the portability of Ada programs to a variety of data processing systems" (par 1.1:1) it also "specifies permissible variations in the effects of consituents of a program unit" (par 1.1.1:16) where "the operational meaning of the program unit as a whole is understood to be the range of possible effects that result from all these variations, and a conforming implementation is allowed to produce any of these possible effects" (par 1.1.1:16). So although the portability between the SUNS and the PS/2's might have been expected (given the AJPO conformance testing procedures), the assumption that a given program will exhibit identical behaviour across various platforms cannot be made and is not implied by the standard.

There are, of course, RISKS here.

Paul ... (Paul Murdock, Paul Scherrer Institute, 5234 Villigen. Switzerland. murdock@cageir5a, murdock@cvax.psi.ch)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Playboy jammer who jammed Hefner's 'jamas gets jammed

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 19 Nov 1990 14:47:24 PST

Many moons ago there were several up-link spoofings, including Captain Midnight interrupting HBO to protest signal scrambling. (See <u>RISKS-2.49</u>, <u>RISKS-3.24</u>, SEN 11 3, 11 5.) As a result of that case, the U.S. Congress passed a law making satellite hacking a felony. The first person convicted under that law is Thomas M. Haynie, an employee of the Christian Broadcasting Network (CBN) who preempted the Playboy Channel in 1987 with a religious message. (See <u>RISKS-5.36</u>, SEN 12 4.) The detective work to identify the culprit used a form of electronic fingerprinting to identify the character generator as a Knox K50, of which only five were located in satellite ground stations. Sentencing is set for 7 Dec 90, with the max being 11 years in prison and \$350,000 in fines. [Update culled from IEEE The Institute, December 1990, p.6.]

✓ Telephone cable cut eliminates O'Hare tower communications

<cook@csel1.eng.ohio-state.edu> Mon, 19 Nov 90 09:58:32 EST

>From the New York Times:

Severed Phone Line Disrupts Chicago Zone

A contractor planting trees severed a high-capacity telephone line in a Chicago suburb yesterday morning, leaving 150,000 people without long-distance and most local telephone service and disrupting businesses across a wide area.

Teller machines at some banks were paralyzed, and flights at O'Hare International Airport were delayed because the air traffic control tower there temporarily lost contact with the main Federal Aviation Administration air traffic control centers for the Chicago area. The Illinois Bell Telephone Company said the line was accidentally cut at 10:02 AM, Central daylight time, and cautioned that full service would not be restored until midnight.

About half the calls blocked by the severed cable were being electronically routed around the break by mid afternoon, said Michael E. LeBeau, an Illinois Bell Official.

People calling telephones with area code 706 in the affected towns recevied a "fast, busy signal," said Gloria A. Pope, a spokeswoman for the utility.

Some flights at O'Hare were delayed by up to two hours but safety was not affected, said James A. Dermody, a spokesman for the F.A.A.

The New York Times (National Edition), Tuesday, 16 October 1990, page A14.

Commentary:

Numerous functions and services in large, complex, systems may be dependent on apparently distant or unrelated events. Such large systems intrinsically have 'latent failures' within them, i.e. failures which are only apparent under a specific set of (often obscure) triggering conditions [Reason J, Human Error, Cambridge U. Press, 1990].

The combination of the contractor digging, the location of the cable, the signals routed through it, the nature of the use of those signals, the time of day, and a host of other factors must join in confluence in order to produce the outcome. Other large systems failures, including Three Mile Island, the Vincennes, the Stark, Challenger, and especially Apollo-13, display this same confluence of (apparently) unlikely events and conditions. The current state of understanding of complex system failures [cf. Rasmussen J, Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering. New York: North-Holand, 1986] and complex system successes [cf. Rochlin GI, et al., The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea, Naval War College Review, Autumn, 1987, pp.76-90] is that failures are virtually never the result of a single fault and that arguments about the nature of causality which focus on single faults mistake the intrinsic nature of these systems. The disasters which arise in complex systems nearly always have an apparent trigger (e.g. captain's failure to

follow procedures for ship navigation) but the event produces disastrous consequences only in a particular setting (i.e. limited navigation tools, schedule pressures, limited manning levels, faulty communications links, faulty superveilance) and that removing the possibility of the particular trigger event does not markedly enhance system safety [for a good example, read the complete report see Marine Accident Report, Grounding of the U.S. Tankship Exxon Valdez on Bligh Reef..., NTSB/MAR-90/04, Washington, D.C.: National Transportation Safety Board, 1990]. Similarly, the recent Hubble telescope issues are gradually becoming focussed on the nature of the project as a large system rather than on the single test/single fault approach [Waldrop MM. Hubble:The Case of the Single Point Failure. Science 1990, 249: 735-6].

The issues of complex, high-risk/high-reliability system failures arise in numerous disciplines, almost all of which rely on computers to provide information to human operators. Faults and failures of such systems produce intense pressures to modify the system components in such a way as to forestall their recurrence. Unfortunately there is little evidence that these pressures are effective in increasing overall system safety [Bowman E, Kunreuther H. Post-Bhopal Behavior at a Chemical Company. Journal of Management Studies, 1988, 25:4]. Large systems represent such significant investments that they are difficult to abandon [Ross J, Staw BM. Expo 87: An Escalation Prototype. Administrative Science Quarterly, 1986, 31:274-297] and it is very difficult to know that retroengineering has produced a markedly more reliable system. The Shuttle may be an example of such a system. It represents a such a large component of the space program that scrapping it and starting over is virtually impossible and there is certainly no guarentee that any new system would not be equally fragile. A rare example of abandonment of a large technical system in favor of another design for primary safety reasons is the new generation of nuclear power generating systems [Golay MW, Todreas NE. Advanced Light Water Reactors. Scientific American, April, 1990], although the technical features of these 'intrinsically safe' plants are difficult to assess.

Arguments about whether a computer is 'expert', or 'advising' human operators are unlikely to produce much useful progress towards developing safer large systems. Indeed, these arguments tend to results in polarized discussions about the roles of technological elements versus the roles of human operators which are little more than the sort of 'hunt for proximal cause' which is described above. The risks of large, computerized system failures are those which accrue to the system rather than to the components. It is clear, however, that pressures during design to meet specific performance, economical, or political requirements may lead to designs which are destined to operate near the extremes of the safety envelope. These pressures, in turn, lead to systems designed to perform more and more at the edge of the safety envelope [Andrewa EL. Sensing the Presence of Potential Problems. New York Times, Sunday 6 May 1990, p.F6]. [Andrews?]

It is particularly instructive to examine the roles of human operators in these systems as they are actually practiced by the operators (rather than as they are defined by rules and procedures, doctine, etc.). In many, even most, such systems, the operators are highly skilled individuals who have developed novel and often quite elegant means for achieving system performance with tools which are only partially suited to the purpose. For example, aircraft pilots modify their environment in a number of ways, including hanging notes on the consoles with paper clips, using the flight management systems in unorthodox ways to plan their flight, etc. Anesthesiologists modify their equipment configurations to preserve certain, critical features of the data display in order to maintain specific relationships on the screen [Cook, et al., The Natural History of Introducing New Information Technology into a High-Risk Environment. Proc. of the Human Factors Society 34th Annual Meeting. Santa Clara, CA: Human Factors Society, 1990, pp. 429-433]. These adaptations are a source of information about the nature of operations, system critical performance areas, etc. and may provide means for improving system feartures in order to produce more robust systems [Hollnagel E. The Design of Fault Tolerant Systems: Prevention is Better Than Cure. 2nd European Meeting on Cognitive Science Approaches to Process Control, Sienna, Italy, 24-27 October, 1989]. Remarkably, operators usually understand the system performance in ways which the designers do not, and achieve safe and efficient operation through various means.

The loss of telephone connection is a particular kind of fault in a large system, one which stresses various system elements in various ways. In this case, it did not apparently cause any airplane crashes, destroy any bank records, etc. But it is particularly instructive to consider what the nature of the arguments would be if there had been an incident at O'Hare, say the collision on the ground of a taxiing and landing aircraft, or a near miss because the handoff to air traffic control was blocked. In these cases the communications system would have come under intense scrutiny (much as did the one in Valdez after the Exxon tanker disaster). What is fascinating about computer associated risks, at least to some, is that some components of the system are resilient and flexible in ways that minimize the effects of component failures. Much of this flexibility resides in the human operators of complex computerized equipment and much of the obstacle to improving safety and mimizing computer-associated risks depends on the care with which computer system designers produce devices which meaningfully enhance that flexibility.

> Richard I. Cook, M.D. Cognitive Systems Engineering Laboratory The Ohio State University

[Don't forget the classical case of logical redundancy compromised by a lack of physical redundancy, the ARPANET routing between NY and New England via 7 logical circuits, all of which went through the same fiber-optic cable, and all of which were cut in one swell foop on 12 Dec 86. (See <u>RISKS-4.30</u> and SEN 12 1, January 1987.) PGN]

Tomatoed 911 (<u>RISKS-10.60</u>)

Rob Boudrie <rboudrie@xenna.encore.com> Fri, 16 Nov 90 17:48:58 EST

A recent posting described an answering machine, without any dial-out capability, which somehow managed to dial 911 when juice from a decaying tomato dripped on it.

there was speculation about undocumented "autodial" features in the phone. I have an alternate explanation:

Although most modern telephones use DTMF (tone) dialing, some older phones use "pulse dialing", in which the circuit is broken in rapid sequence [In my younger years, I used to be able to dial any number on a telephone by banging on the switchhook - I did this just in case the dial broke, not so I could dial out from phones with locks on the dials :)]. Modern telephone switches recognize both pulse and DTMF dialing, except where DTMF tones are filtered out for customers who don't pay a surcharge for DTMF service.

So...It is very possible that the tomato juice was causing some sort of electrical condition that resulted in the machine rapidly going on and off line in an intermittent manner. Although unlikely, it is possible that this resulted in 9 rapid on/off cycles, followed by two single on/off cycles at a lower pace.

Rob Boudrie

rboudrie@encore.com

Computer-Aided Gerrymandering

<scs@ATHENA.MIT.EDU> Sun, 18 Nov 90 14:16:02 -0500

Naif that I am, I always thought that gerrymandering was a "bad word," a practice that no modern thinking person would speak of except to denounce. Wrongo. Under the headline "GOP hopes high tech will give it edge in redistricting", the Boston Globe (November 18, 1990, page 5) mentions "how bad the GOP has been at gerrymandering in the past" (i.e. that they did it ineffectually, not egregiously) but that they "have learned a lot about redistricting in the intervening nine years."

"There's no big secret about this; we haven't been very good in the last few decades at this redistricting game," [political director of the Republican National Committee Norman] Cummings said in an interview. "You'd always like more, of course, but we're in much better shape now compared to 10 years ago... and the Democrats could be in for a surprise before it's all over."

After discussing the implications of the shifts in party balance due to the recent elections, the article finally gets to the "high tech" part, describing how the Republicans "plan legal assaults, assisted by new computer capabilities."

This strategy is based mainly on the Civil Rights Act of 1982, which mandates that districts with a majority of blacks, Hispanics, or other minorities must be drawn wherever possible.

With that in mind, the GOP has devised software allowing anyone with a computer to draw alternative lines and has arranged for civil rights groups to obtain it for free. The intent is for minorities, who tend to vote Democratic, to be grouped together, leaving more Republicans in adjoining areas. "What the Republicans want to do is go in and create one black district that will result in weakening three or four Democratic districts to make them Republican or at least competitive," said Howard Schloss, spokesman for the Democratic Congressional Campaign Committee.

Neat trick; use a law which was intended to protect minorities, when they had less political power, against them now that they have more; and dangle bait (the software) which will let them do your job for you. It may be working:

An initial foray into tinkering with minority districts, partly by using the GOP's software, was to be made this weekend in Texas by several groups whose function is to get more minorities involved in the political process; they include the Southwest Voters Project and the Mexican-American Legal Defense Fund.

Those organizations' work has tended to benefit Democrats in the past, but Republican officials hope that is about to change.

"Both minorities and the Republican Party have been the victims of gerrymandering by the Democrats," said Benjamin Ginsberg, the Republican National Committee's chief legal counsel, who plans to attend the strategy session in San Antonio. "So this is a natural alliance for the redistricting process."

Once again, the underlying RISKs are as old as the hills, but a bit of computer assist can allow them to be exploited ever-so-much-more-so effectively.

Steve Summit

scs@adam.mit.edu

✓ GOES mirror problems caused by oversimplified analysis

<henry@zoo.toronto.edu> Sun, 18 Nov 90 17:37:52 EST

Catching up on my reading, I found a very interesting piece in the Aug 13 issue of Aviation Week & Space Technology. The next series of GOES weather satellites are experiencing serious development problems: the main mirrors of their imaging systems warp when exposed to extreme temperatures. (To head off the inevitable question: this is *completely* unrelated to the Hubble telescope's mirror problems.) To quote:

The design for the new mirrors was derived from Ford [prime contractor] and ITT [instrument subcontractor] experience in developing smaller mirrors for the Indian Insat spacecraft. A computer model of the mirrors initially used to verify their stability showed that they were designed properly. That model was based on 30 data points across the mirrors.

But during thermal vacuum testing in late 1989, when the mirrors were integrated with the sounder and imager telescopes,

the instruments began to show anomalies... [initially thought to be possibly due to other problems].

ITT engineers were not completely sure what caused the problem, however, so they devised a more complex computer model of the mirrors that used 1600 data points instead of 30. The improved tests showed that the mirrors had a thermal warpage problem...

This adds to the problems of the new GOES series, which is already far over budget and two years behind schedule. The schedule is starting to look like a major problem, because NOAA is already down to one operational satellite in orbit, and two are really needed for full coverage of the Americas. Originally the first replacement was scheduled for launch this year, but now even the current target of Feb 1992 is looking optimistic.

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

Privacy concerns about new Lotus "Marketplace" product

Dan Aronson <dan@big-ben.UUCP> Fri, 16 Nov 90 11:38:37 PST

Lotus claims that if you don't want to be in the database you can write a letter to:

Lotus Development Corp. Attn: Market Name Referral Service 55 Cambridge Parkway Cambridge, MA 02142

--Dan Aronson, Thinking Machines Corporation

[Also noted by noah@cs.washington.edu (Rick Noah Zucker)]

* AFCEA's 2nd Annual Military / Government Computing Conf/Exp

Jack Holleran &olleran@DOCKMASTER.NCSC.MIL> Fri, 16 Nov 90 14:16 EST

AFCEA's 2nd Annual Military / Government Computing Conference and Exposition Dates: February 5-7, 1991 Location: Hyatt Regency, Crystal City, Arlington, VA

Additional Information: The Armed Forces Communications and Electronics Association 4400 Fair Lakes Court Fairfax, Virginia 22033-3899 (703) 631-6225

Theme: Information Systems Solutions Today & Tomorrow

Concurrent tutorial sessions will be presented on February 5; Four technical tracks will be presented on February 6-7. Technology Advances (February 6); Information Systems Applications (February 7); Software Development / Maintainence (February 6-7); and Systems Security Solutions --- Security / Privacy, Integrity and Availability (February 6-7).

February 5, 1991 Concurrent Tutorial Sessions Tutorial Co-Chairmen Mr. Larry Walker, Director, Command Control and Planning, CONTEL Federal Systems LTC Calvin Hastie, USA Office of the Director of Information Systems C4 Headquarters, Department of the Army, Army Management Division

- Open Systems Architecture
 Improving the Software Process
 Mr. J. Mogilensky, Director of the SW Process Enhancement Program,
 CONTEL Federal Systems
 MLS-A Critical Technology
 Col. Bill Freestoner, USA, Program Manager
 Defense Communications Agency
- II Expert Systems in Artificial Intelligence Imaging / GraphicsPersonal Authentication Via Biometrics
- III Evolutionary Systems Acquisition
 D. Shore, Technical Director, AFCEA
 Dr. S. Starr, The MITRE Corporation
 Dr. S. Albert, Vice President and Chief Scientist,
 Institute for Systems Analysis
 Information Engineering
 Mr. J. Weyland, Senior Associate, Booz, Allen & Hamilton, Inc.

Technology Advances (February 6, 1991) Track Co-Chairmen: Dr. Paul Oliver, Vice President, Booz, Allen & Hamilton, Inc. Mr. John Carabello, Dean, Information Resources Management College, National Defense University

- * Artificial Intelligence and Expert Systems Moderator:
 Dr. Larry Medsker, Chairman, Computer Science and Information Systems, American University
- * Imaging and Graphic Systems
 Moderator:
 Dr. Alan Salisbury, President, CONTEL Technology Center
- * Information Engineering Moderator:
 Mr. Jon Whalen, Senior Associate, Booz, Allen & Hamilton, Inc.

Information Systems Application (February 7, 1991) Track Co-Chairmen BGen J. Ronald Carey, USAR Program Manager, Reserve Component Automation System, National Guard Bureau Mr. Thomas L. Hewitt, President Federal Sources, Inc. * Panel: Managing Large Systems BGen. John F. Phillips, USAF, Commander Logistics Management Systems, Air Force Logistics Command Wright-Patterson AFB Mr. Edward G. Lewis, Assistant Secretary Information Resources Management, Department of Veteran Affairs Mr. Frank DeGeorge, Inspector General, Department of Commerce Mr. Robert Cook, Chief Executive Officer The Systems Center * Wrap-up of the 101st Congress and Expectations for the 102nd Congress on Issues and Legislation Effecting Information Technology Application Presenter: Mr. Steven Ryan, Attorney, Former General Counsel for Senator John Glenn's Government Affairs Committee * A Success Story of How USAA Achieved a Paperless Office with Information Technology Presenter: MGen. Donal Lasher, USA (Ret.), Senior Vice President, **USAA** Insurance Company * A Successful Turnaround in a Major Government Application Presenter: Mr. Thomas P. Giammo, Assistant Commisioner for Information Systems, U.S. Patent & Trademark Office, Department of Commerce * The United States Postal Service in 1995 Presenter: Dr. Bernard J. Bennington, Director of Communications and Technology, **U.S.** Postal Service Software Development / Maintenance (February 6-7, 1991) Track Co-Chairmen: Mr. Anthony M. Valetta, Program Executive Officer Standard Army Management Information Systems, Department of the Army Mr. John Turner, Associate Administrator, National Aerospace System Development, Federal Aviation Administration * Maintaining Quality in the Software Development

Presenter: Mr. James Emery, Professor of Decision Sciences,

Wharton School of Business

- * Grand Design vs Evolutionary Development / Acquisition
- * Panel: Prototyping Moderator: Dr. Michael F. McGrath, Director of CALS Office, Office of the Assistant Secretary of Defense
- * Panel: Managing the Corporate Information Management (CIM) Life Cycle Moderator: Mr. John Gioia, President, Robbins-Gioia, Inc.
- * Panel: Modernization / Uptrade / Re-engineering Moderator: Dr. Paul Oliver, Vice President, Booz, Allen & Hamilton Panelists: Mr. Phil Kiviat, Vice President, Chartways Technology Mr. George Baird, Senior Associate, Booz, Allen & Hamilton
 - Mr. Roger Kerchaw, Program Director,
 - Educational Testing Services
- * Panel: Maintainability
 - Modeator: Mr. John Caron, Assistant Commissioner, Office of Technical Assistance, General Services Administration
- * Panel: Software Re-Use
 Moderator: Mr. Mitchell J. Bassman, Senior Scientist, Special
 Projects Division, Computer Sciences Corporation
- * Panel: Ada
 Moderator: Dr. Clay Stewart, Associate Director, C3I Center George Mason University
 Panelists: Dr. Win Royce, TRW
 Mr. Paul Mauro, Hughes

Systems Security Solutions Security / Privacy, Integrity and Availability (February 6-7, 1991)
Track Co-Chairmen:
Mr. Patrick Gallagher, Director
National Computer Security Center, National Security Agency
Mr. James H. Burrows, Director of National Computer Systems Laboratory
National Institute of Standards and Technology

- * Panel: Computer Security Applications Experiences: National Security Moderator: Mr. Patrick Gallagher, Director, National Computer Security Center, National Security Agency
- * Panel: Computer Security Applications Experiences: Civilian / Commercial Moderator: Mr. James H. Burrows, Director of National Computer Systems Laboratory, National Institute of Standards and Technology
- * Panel: Computer Security Procurement Experiences
 Moderator: Ms. Barbara Guttman, Computer Specialist, National Institute of Standards and Technology
 Panelists: Mr. Hal Tipton, Director and Past President,

Information Systems Security Association (ISSA), Inc.

- * Panel: Voice / Data Security Applications Moderator: Mr. Ray Fitzgerald, Central Intelligence Agency Chairman: STS/SISS Joint STU-III Working Group
- * Panel: Network Security --- Applications Moderator: Mr. Curt Barker, Senior COMSEC Analyst, Trusted Information Systems, Inc.
- * Panel: Protection Against Malicious Software Moderator: Mr. Dennis Steinauer, Manager of Computer Security Management and Evaluation, National Institute of Standards and Technology
- * Panel: Where are We Going? Moderator: Mr. Steve Walker, President Trusted Information Systems, Inc.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<mrotenberg@cdp.uucp> Mon, 19 Nov 90 22:20:17 -0800

I think Lotus got off easy in the Wall Street Journal story (11/14/90, B1). The reporter did not pursue the interesting and novel privacy issues with the Marketplace product. For example, the "opt-out" approach will probably not work with a list published on CD-ROM. How does a person remove a name once the product is available? Also, once the data is in digital form isn't matching against other databases, such as phone directories, more likely? Traditionally, mailing lists were exchanged in paper formats and available only for one-time use.

These are a few of the reasons that I disagreed with the comment in <u>RISKS 10.61</u> that the privacy debate is on familiar grounds. This is the first

time that a company has prepared to sell a large consumer database on CD-ROM. This raises new privacy issues and new risks that should be evaluated before the product is sold.

Another interesting point about the Marketplace product -- no restrictions on previewing sets. You are charged when you print labels, but not when you view sets on the screen. The product also allows piping to other application programs.

And here's the interesting risks problem: Lotus has said that the encryption scheme will prevent individual record access. Brute-force searching will almost certainly work since there are no charges for previewing a list, but it's slow for searches on multiple record subjects. So, what is the likelihood that someone will break the encryption scheme?

Marc Rotenberg, CPSR Washington office.

✓ Lotus MarketPlace brochure

Eric Dittman <dittman@skbat.csc.ti.com> Tue, 20 Nov 90 17:56:15 -0600

I received a brochure on Lotus MarketPlace the other day in the mail. Nowhere in the brochure is there mention of any limit to the distribution of the database. According to what I have read in the brochure, both MarketPlace:Business and MarketPlace:Households will be available at dealers, so anyone should be able to buy MarketPlace.

Eric Dittman, Texas Instruments - Component Test Facility

Insurance Perfidy [forwarded]

<34AEJ7D@CMUVM.BITNET> Tue, 20 Nov 90 09:11:01 -0800

Written by: CREGIER@UPEI.CA (Sharon Cregier) [Reprinted with permisson -- see copyright notice at end of article]

Computer records, even erroneous ones, allow insurance companies to discriminate against applicants and clients. The following is a copy of an article in the August 1, 1990 issue of the Christian Science Monitor (Boston) article, FROM DATABASE TO BLACKLIST, section heading: Insurance risks targeted.

Perhaps one of the most mysterious consumer-reporting companies is MIB, formerly the Medical Information Bureau, in Brookline, Mass. "It's a very difficult company to learn very much about," says Massachusetts state senator Lois Pines. "They don't want people to know that they exist or what they do."

"The purpose of MIB is to help keep the cost of insurance down for insurance companies and for consumers by preventing losses that would occur due to fraud or omissions," says MIB's president, Neil Day. MIB's files are used by more than 750 insurance companies throughout the United States and Canada.

MIB stores its records in a specially coded format, which the company refuses to share with regulators, legislators, or consumer groups. There are codes for medical conditions and mental health, as well as nonmedical conditions like "hazardous sport participation" and "hazardous driving records."

In the past, says Robert Ellis Smith, editor of the Privacy Journal, other MIB codes have stood for "sexual deviance" and "sloppy appearance." Mr Day refuses to release a list of the current codes used by his company, saying that to do so would compromise his firm's confidentiality.

Although MIB will tell a person if he or she has medical records on file, it will send those records only to a medical professional. The company receives 15,000 requests by individuals to have their report sent to their physician every year, says Day. Between 250 and 300 people argue with their reports.

A person applying for life insurance enjoys none of the privacy rights and protections that a person applying for credit does, says Josh Kratka, an attorney with the Massachusetts Public Interest Research Group (MASSPIRG).

"MIB has agreed to abide by [the FCRA]. They will send those codes to your physician. Your insurance company is not under those obligations....If you are denied life insurance, you have no way of knowing whether it was legitimate or based on an error in your records that is going to follow you around for the rest of your life," says Mr Kratka.

In one case, says Kratka, a Mass. man told his insurance company that he had been an alcoholic but had managed to remain sober for several years and regularly attended Alcoholics Anonymous meetings. The insurance company denied him coverage and forwarded a code to MIB: "alcohol abuse; dangerous to health."

The next company the man applied to for insurance, Kratka says, learned of the "alcohol abuse" through the information bureau and charged the man a 25% higher rate.

In another case he says, a clerical error caused a woman's records at MIB to say that she carried the AIDS virus. "It was only after unusual intervention by the state regulatory board," because the woman worked for a physician, that the records were corrected, Kratka says. MASSPIRG has filed state legislation that would extend many of the FCRA's protections to medical records.

As health-care costs continue to rise, say experts, consumers can expect less and less privacy regarding their medical records.

"Doctors, in order to get paid, are being asked more and more to identify a chargeable condition in their clients....The breach in confidentiality is a natural consequence of the way in which third party billing of physician's time is structured in this country," says Dr Paul Billings, chief of genetic medicine at the Pacific Presbyterian Medical Center in San Francisco.

No federal law ensures the confidentiality of medical records. Some hospitals, Mr Smith says, have even started using them for target marketing.

Reprinted with permission from the Christian Science Monitor Copyright 1990 by the Christian Science Publishing Society, All rights reserved

// [anonymous] author identifies anonymous referee

<[anonymous]> 20 Nov 90

I'm not sure if this is a technology-based risk or a process-based one.

Recently, I had a paper rejected from a technical conference. As usual, the committee returned to me the reviewers' comments with the identifying header removed. However, they neglected to remove the small line of type placed at the head of the page by the reviewer's fax machine. This machine kindly gave me the reviewer's place of employment (down to the building and department names) and fax number. Better than caller ID, since I can correlate that with the (small and public) list of reviewers for this conference and arrive at the reviewer's name.

We can see this as a technology-based risk in that the reviewer didn't know that his identifying information was going to be publicized. Or we can see it as a process-based risk in that no one involved remembered to remove the identifying line (and that the reviewer was in a sufficient hurry that he used the fax rather than another transport medium).

Keuters Holdings PLC and shouldering the blame? [Abstracted by PGN]

Sameer Mithal < Wed, 21 Nov 90 07:12:23 PST

An article entitled ``Who takes the blame when trades short-circuit?'' in the Wall Street Journal, 20-Nov-90, p. C1, discusses the problem the general problem of how to resolve liability questions in case transactions are messed up by computer-related screwups. In particular, pending resolution of the liability issue, Reuters Holding PLC has announced an indefinite delay in the development of Dealing 2000-2, a network of systems for foreign-exchange trading. Clearly Reuters would like to limit their risks. The article is not overly informative, but does sound the English horns of the dilemma. [PGN]

MD-11 test flights over the pole

<henry@zoo.toronto.edu> Sun, 18 Nov 90 23:05:09 EST

Interesting item in the 22 August issue of Flight International: the prototype of McDonnell-Douglas's new MD-11 airliner (a DC-10 derivative) made a test flight partly aimed at testing performance of navigation software in the vicinity of the North Pole, making four passes directly over the pole and one nearby. On two of the pole passes, the flight-management computers were

deliberately "failed" to see if the backup equipment would function. No problems, they say.

(This is not as trivial as it sounds, because the vicinity of the poles is a severe worst case for navigation algorithms. The distance between degrees of longitude goes to zero while latitude remains unaffected, trig functions are pushed to extrema of their behavior, and there is a singularity in the coordinate system at the pole itself.)

Henry Spencer at U of Toronto Zoology

* Soc.Sec.No. on Driver's Lic. (was Re: Sprint's New Calling Card)

William Ricker <wdr@wang.com> Mon, 19 Nov 90 20:23:54 EST

Jerry Glomph Black, black@MICRO.LL.MIT.EDU writes: >Even the police-state People's Republic of Massachusetts allows you to specify >a bogus SS No. for your driver's license, instead of your real one, so long as >your bogus no. doesn't duplicate somebody else's license no.

Bad news -- the Mass. Registry of Motor Vehicles now requires that their computer contain your SSN as well as your bogus number. I requested and was given a "S-number", an 8-digit number with an S prefix, as my drivers license number years ago. but on my most recent birthday -- election day, this month --I was informed that to renew, I must supply my SSN in confidence to the computer, but not to worry, it wouldn't be printed on my license. Yes ma'am, it is your computer that I don't want to have it.

I protested ... and was informed by Registry's legal department that Mass. Law overrides any federal law, and if I didn't want to comply, I didn't have to renew my license to drive, did I?

The Mass chapter of the ACLU has informed me that the Mass. RVM has the right to demand this number from me. I must call them back and get the chapter and verse on that; I would like to see a full opinion.

One angry camper,

/bill ricker/ wdr@wang.com a/k/a wricker@northeastern.edu

Tomatoed 911 (Boudrie <u>RISKS-10.62</u>, re: <u>RISKS-10.60</u>)

Tim Steele <tjfs@tadtec.uucp> Tue, 20 Nov 90 17:52:00 GMT

[...] My best guess at What Really Happened is:

The answering machine does in fact have a built in phone (otherwise why would it be able to dial?)

The phone probably has a memory button programed to dial 911.

The tomato juice probably dripped on to the button and 'shorted' it out (the dialler chip is probably expecting a rubber membrane keyboard and will accept a fairly high resistance as a valid key press.

Tim



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Alan Jeffrey <jeffrey@cs.chalmers.se> Sat, 17 Nov 90 12:56:52 +0100

There is an additional risk associated with voting from home, not mentioned by any of the posters. By making it easier for people with phones to vote, you are helping to disenfranchise those who can't afford phones. I don't know about the US, but in the UK telephone voting would (perhaps significantly) boost the results of the ABC1 / over 35 / Conservative vote, with resultant damage to the Labour party.

If we're going to claim to live in representative democracies, we're going to have to make the technology for voting equally available to all.

Alan Jeffrey 031 721098 jeffrey@cs.chalmers.se

Computer Science Department, Chalmers University, Gothenburg, Sweden

Ke: Voting electronically from home (revisited)

<smb@ulysses.att.com> Fri, 16 Nov 90 13:40:30 EST

> From: li@diomedes.UUCP (Li Gong) ... I would like to add that the current system not only provides physical security of identification, but also physical security against harassment. Nobody else is allowed to go into the booth when a voter, say Alice, is voting inside.

You overassume. In *theory* no one else is allowed to go inside the voting booth (subject to a few exceptions for illiterate or handicapped voters, btw); practice is something else entirely. I still recall my astonishment the first time I witnessed the quaint local voting customs in Durham, North Carolina. A husband and a wife would enter the booth together, and cast a vote; the wife would then exit, and the husband would vote (again?).

Then, of course, there's Chicago, a town that gives entirely new meaning to the phrase ``voting machine''.... But I digress.

--Steve Bellovin

Mecoming over-sensitive to risks (vote by phone)

Brad Templeton <brad@looking.on.ca> Sun, 18 Nov 90 3:19:13 EST

While I appreciate people's concern over the sanctity of the vote, consider what is used now.

I don't know about the U.S., but in Canada there's almost no security on voting. They come round to your house every election, and ask for the names of every elector. No ID is asked for. You could name your children or pets and they would get on the voters list. (It's no doubt a crime of some sort to do this, of course.)

Likewise all you have to do is go to the poll, and give the name of any person who hasn't voted yet (normally yourself.) As long as it isn't a small poll, you could easily use any other name. (The lists are posted on telephone polls so people can check they're on.) If you have good eyes and can read upside down, you can even look at the RO's name sheet when you walk in.

Sounds ripe for fraud, but it just never happens. When a seat is hotly contested or close, the party scrutineers watch things closely, in addition to the elections officials. I have never heard of any accusations of abuse.

While using SSNs or other publicly available info isn't a good idea, I would have no opposition to well designed phone voting -- particularly in an area with ANI. There are RISKS, but as long as we watch for them, they are no

greater than those of the current system. The greatest RISK is not watching for RISKS because we trust the computer too much.

On the other hand, there are other problems with phone voting -- the largest being the elimination of the secret ballot. The voting computer will know who voted for whom. We must trust the programmers and their auditors to assure us the information is erased and never stored. (On the other hand, doing this disallows one great method of verifying phone voting, namely a mailed ACK.)

Brad Templeton, ClariNet Communications Corp. -- Waterloo, Ontario 519/884-7473

Ke: Voting electronically from home (revisited)

<henry@zoo.toronto.edu> Sat, 17 Nov 90 19:19:12 EST

>... in the most recent election, I found myself rushing
>to the polling place near my home... and arrived too late. If I could have
>voted at a location near my work, or by telephone, problem solved.

There are several simple non-technological fixes for this, notably the one followed in a number of other countries: hold elections on Sundays, when most people have at least part of the day free.

Henry Spencer at U of Toronto Zoology utzoo!henry

[An eminently reasonable suggestion, although we have drifted away from the computer relevance -- except that you have found a very simple nontechnical solution to the problem. PGN]

Voting by phone

silva <peter@ficc.ferranti.com> Sat Nov 17 08:42:17 1990

> [use Caller-ID to] foil attempts by people to cast large numbers of votes> from one phone, even if the authentication system were compromised.

This would tend to disenfranchise people in poor neighborhoods where there may only be a single public phone to serve an entire apartment block.

Also, it would be desirable to have the call to the election service be free in areas with measured service or from a pay phone. And of course the dangers of COCOTs (private pay phones) would be increased.

Another contributer noted:

- > For example, in the most recent election, I found myself rushing
- > to the polling place near my home (since you can only vote at
- > the registered polling place) and arrived too late. If I could have

> voted at a location near my work, or by telephone, problem solved.

A simpler and less dangerous solution would be to allow you to vote at any polling place, and have some form of real-time communication between the polling places to prevent fraud.

Another negative effect I could imagine would be that this would enable proxy voting: "You're a good Republican, and you just want to vote the straight party ticket.

"Call 1-800-VOTE-GOP" or "1-800-VOTE-DEM" and have your election ID number at hand...

Peter da Silva. +1 713 274 5180. peter@ferranti.com

Voting by phone

P.J. Karafiol <karafiol@husc8.harvard.edu> Sun, 18 Nov 90 23:34:53 -0400

With all this talk about vote *fraud* I'm surprised no one mentioned a serious, actual *infringement* on one's constitutional rights. If voting is done by phone, what happens to people who don't have one, either because of location (yes, there are places in the continental US without regular phone service, although all the ones I know of are reachable through some kind of radio-phone system) or finances or personal choice? Although poor or phone-phobic people could conceivably use a public phone (the number would presumably be toll-free) it still seems unfair to people who are in category 1. Questions, comments, discussion?

Caveat: I didn't read the original (non-electronic) article on voting by phone. This concern may be addressed in that article. == pj karafiol

Voting from home (Re: <u>RISKS-10.61</u>)

Barbara Simons <simons@IBM.com> Sun, 18 Nov 90 22:59:34 PST

In discussing voting electronically from home, Li Gong says (in <u>RISKS DIGEST 10.61</u>):

I would like to add that the current system not only provides physical security of identification, but also physical security against harassment. Nobody else is allowed to go into the booth when a voter, say Alice, is voting inside. On the one hand, this gives Alice privacy; on the other, she can vote according to her own will. Moreover, since this individual vote is among maybe a billion other votes, no ordinary person could find out for whom Alice has voted. This potentially discourage "buying" votes with money or menace, because it is difficult (if not impossible) to "physically" influence a voter at voting time and/or to verify a voter's vote afterwards. He then goes on to mention that he and his former advisor had been working on a zero-knowledge method for voting. This is an interesting idea, but it assumes an outsider who wishes to know about or influence Alice's vote. Suppose, however, that her husband has decided how he wants Alice to vote. In most states, he would not be allowed into the voting booth while she voted. But he could easily watch her as she votes electronically at home.

The risk in this situation is that an obvious form of intimidation has not been taken into account.

I said that in most states he would not be allowed into the voting booth while she voted. I recall hearing about some Southern state in which a husband and wife are (were?) allowed into the voting booth together. Apparently, the theory was that the husband would vote for them both. Unfortunately, I don't recall the state nor whether this unhappy situation still exists.

Barbara

Ke: Voting electronically from home (revisited)

Joseph R. Beckenbach <jerbil@tybalt.caltech.edu> Mon, 19 Nov 90 20:37:29 GMT

Why am I still under the impression that this "vote-by-phone" is a technical solution to a nontechnical problem? True, a "vote-by-phone" system would be useful for hospital patients and shut-ins of many sorts, but absentee ballots were made for this, were they not?

Why not simply declare Election Day a national holiday? We celebrate the Fourth of July in the USA because it reminds us of past efforts to keep freedom. Why not one to remind us of our duty to safeguard current freedoms?

When I form a company, I intend on making Election Day a half-day or full-day holiday with pay, with proof of vote. Or some other scheme which penalizes for not voting if the person is eligible. [I'd rather not reward for performance of a duty, but if such is necessary, I will.]

Joseph Beckenbach

Re: Voting electronically from home

&lan_Marcum@NeXT.COM> Tue, 20 Nov 90 17:05:49 PST

Imagine how much havoc a vote-by-phone system would wreak on dear Ma Bell out here in California, the Land of the Ballot Proposition. Millions of hour-long telephone calls as citizens try to register their votes on the dozens (yes, literally) of propositions. "We're sorry, your call did not go through. All voting circuits are busy now. Please try again tomorrow..."

Alan M. MarcumNeXT Technical SupportAlan_Marcum@NeXT.COM+1-415-363-5153

Voting (Re: <u>RISKS-10.61</u>)

K. M. Sandberg <sandberg@ipla01.hac.com> 19 Nov 90 00:27:25 GMT

In regards to voting, it was mentioned that current voting is based on physical security, but at least where I vote all I do is bring in the little booklet and sign the book and I get to vote, no check of who I really am. If I had multiple booklets I could vote several times, but since I must go to one place to vote and sign in I could not vote multiple times based on my own name.

In another response it was said that having the phone system would help voting since the person said that they missed getting to the poles, but absentee ballots solve this if it is a normal problem. The risk of influencing the votes because of the current privacy, unless the absentee ballot is used, is important. Other solutions would be to send the ballot, like the absentee ballots, and allow people to drop them off, but this still has the risk of lack of privacy. Personally it would be nice if you could vote at a common place, possibly before election day, with the same privacy and security, maybe at your local post office or at a pre-selected place to prevent multiple voting. Too bad we can't trust people.

In this last risk posting, it mentioned that people could enter in their votes for practice only so that they would get used to it, but a question that comes up was this information used BEFORE the end of election day? If it was it could have affected voting, as does the exit polls, east coast results before the west coast polls close, etc.

Kemasa.

Re: Election coverage software

Chris Maltby <chris@softway.sw.oz.au> Wed, 21 Nov 90 14:00:24 EST

>The News Election Service, the central clearing house for election>information, has their systems set up to deliver vote percentages that>show the major party candidates' votes adding up to 100%, even when>the major party candidates don't capture 100% (as they usually don't).

I was certainly intrigued by this and other things as I watched the election coverage in Boston. Having worked on the software for the Australian Electoral Commission for the last federal election (March 1990) there I was surprised by the (parochialism speaks) poor standard of the reporting.

First, the results of counting seemed to be very slow to arrive, leaving the

commentators to talk about nothing for long periods. Some districts still had only 1% of precinct reporting at 11pm. In the Australian election, at least 80% of the vote had been counted by 11pm.

Second, there seemed to be no analysis of swings and only minimal discussion of trends in early vs. late figures. The commentators were predicting a win for Weld although he trailed for most of the night. The information they based the prediction on was not produced.

Given that the first-past-the-post system is significantly easier to count than the preferential system in use in Australia, there seems to be little possible excuse for the delay/inaccuracy of the result reporting.

To put things in perspective however, and to reveal the "risk" for this posting, the Australian experience was not without problems. For the first time the Electoral Commission attempted to make predictions based on preliminary results from individual polling booths. That is, when figures for a booth came in they were compared with previous figures from the same booth to yeild a "swing" percentage. This swing would then be propagated over the booths for which no result was yet known. This was expected to be able to give very accurate predictions. The magic quantity is dubbed the "two-party-preferred" vote.

The unknown factor turned out to be the unusually high vote for minor parties and independents, with an even more unusual preference distribution pattern. The preference system allows voters to protest their favourite major party's policy/candidate but direct their second preference to that party ahead of the other major party. This option was exercised in much higher numbers than ever before, and especially among Labor voters. The commission's system made some rather simple assumptions about minor party preferences.

As a result, for most of the night, the prediction was a landslide for the Liberals based on an apparent swing above 10%. The actual result was a solid win for Labor of 8 seats (as predicted by count scrutineers). In two electorates independents were able to beat one major party into second place and win the seat on preference votes.

A better system for preference sampling is being implemented for the next election...

Chris Maltby - Softway Pty Ltd (chris@softway.sw.oz.au) PHONE: +61-2-698-2322 UUCP: uunet!softway.sw.oz.au!chris

Voter registration isn't always pre-registration

<rsimkin@dlogics.UUCP> Mon Nov 19 09:31:07 1990

In <u>Risks 10.61</u> "Re: Voting electronically from home (revisited)", Stephan Meyers says:

> How does this sound: before each election, each voter is mailed a
> confirmation of registration (since, I believe, to vote one must be> registered, and to register, one must have a permanent address)

This assumes that registration must be completed well in advance of election day, which isn't always the case. In the name of making the voting process more accessible, Wisconsin law used to (and may still) allow voters to register at the polling place on election day. As a result many people would arrive at the poll with proof of residence, register, and then vote.

--Rick Simkin

Ke: Voting electronically from home (revisited)

Flint Pellett <flint@gistdev.gist.com> 19 Nov 90 22:49:15 GMT

li@diomedes.UUCP (Li Gong) writes:

>I would like to add that the current system not only provides physical security >of identification, but also physical security against harassment.

This is what I think the biggest risk of vote-by-phone is: Al Capone decides he wants to be mayor, and has his flunkies each call 100 kindly little old ladies in the month before the election, telling them "Come to my house to cast your vote or I'll ..." and then, the flunkies watch the little old ladies punch their votes into the telephone, and make sure they vote the "right" way.

Anyone care to enlighten us on what types of security measure are planned to deal with this type of problem? Merely being able to recognize that you are recording a vote from the proper person is not sufficient. Any scheme with authentication numbers suffers from the fact that it will never be any more secure than the way in which those numbers are communicated to the voter, and the way in which the voter remembers them. (If you have to mail the numbers to the voter, then that mail can fall into the wrong hands. If the voter has to write it down in order to remember it, which is quite likely for most people given that they use it once every 6 months or less, it is also at risk.)

Flint Pellett, Global Information Systems Technology, Inc. 1800 WoodfieldDrive, Savoy, IL 61874(217) 352-1165 uunet!gistdev!flint

Ke: Election coverage software

Gregory G. Woodbury <ggw%wolves@cs.duke.edu> Mon, 19 Nov 90 17:52:18 GMT

Here in Durham NC, we had a rather interesing election :-) It seems that nearly half of the voting machines in the county went haywire and would not work correctly on election day! This happened early and we had a court ruling that the polls stay open to 10pm and that paper ballots be made available in all precincts to those who wanted them. In my precinct (I am an assistant election official) only two of our 6 mahcines had problems and we (hopefully) caught them as soon as they occurred. Even so, our audit numbers were off by 4 at the end of the night. The particulars of the election seem to be that in the county commissioners races, for the first time in xxx years (maybe the first time ever) we had an INDEPENDENT candidate, not in conjunction with an independent running for president. The machines are set up so that one can "split ticket" by pulling the straight party lever and then deselect one candidate and select another. The problem for all the machines that I have been able to get exact information on seems to be that people tried to split ticket and forgot to deselect a candidate before selecting someone in the other parties lines. This jammed the levers in the county commissioners section and rendered the machine unuseable.

Considering that most voters do NOT understand the ways that machines work, it happened in some precincts that the jammed machines where used until someone complained or noticed the jam. This is the RISK. People assumed that the technology would behave correctly. When something did go wrong, they ignored the errors cause they didn't know any better. In this city, however, we have a high ratio of advanced degrees (MS,PhD,etc) in the population in certain precincts, and even there, the problems occurred.

On a side note: when the judge ordered the use of paper ballots AND staying open til 10pm, he made it IMPOSSIBLE for Durham results to be known before 2am! The precincts are set up to deal with a small number of paper ballots (for disabled voters unable to enter the polling location but coming near by in a car - "curbside voters"), but extending these paper ballots to anyone who wanted to use them placed an unexpected load on the pricint officials when the polls closed! I had volunteered monday evening to count paper ballots (before the judge's order) and instead of 25 or so ballots, we had nearly a hundred! That was so much FUN! *HA!*

By the time we finised counting and had the helms/gantt figures for NES it was 3am and they had the time to ask why we were the first precinct from Durham NC to call in "official" results. -- Gregory G. Woodbury

Durham NC UUCP: ...dukcds!wolves!ggw ...mcnc!wolves!ggw ggw%wolves@mcnc.mcnc.org



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Pete Mellor <pm@cs.city.ac.uk> Sun, 2 Dec 90 09:14:27 PST

Sitting up late one night last week, I caught the re-broadcast in the UK of the US news program "60 minutes".

One of the items was about ADATS, a tank-based anti-helicopter missile system, meant to be effective in conditions of poor visibility (e.g., Iraqi sandstorms), and reckoned to be essential against such things as the HIND killer-chopper (of which Iraq is rumoured to have 40 or so). It is, or rather was, being developed by Oerliken of Switzerland. However, they have pulled out, and (I think) the completion of the system is now directly managed by the DoD. This follows cancellations by several potential customers: Germany, Holland, Saudi Arabia, etc. Only the US and Canada still seem to be interested.

It is strongly supported by some military people, e.g., General Granrod (? -Sorry, there were no subtitles, so I wasn't able to get the correct name of everyone interviewed, and I have no idea what any of the acronyms stand for.), who said it had exceeded its requirements in field trials. Convincing film was shown of it shooting a parked helicopter off the top of a tower, and then firing a missile in a corkscrew spiral ending in the nearest bit of shrubbery.

A strong feeling of deja vue then descended, as it turned out that this system is (you've guessed it!) highly computerised.

There seem to have been a few unfortunate hitches in its development:-

Originally estimated at \$7 billion, its cost has now reached \$12 billion and is rising fast. Protests from parts of Congress on behalf of the US taxpayer are the main reason for its current notoriety.

It is late. Certainly too late for the gulf. After having been under development for years, it is still at least 5 years from delivery.

Its requirements seem, err..., less than adequately related to the real world. It uses laser to track its target. This is not a bright idea for an all-weather system. "You don't see through clouds with a laser.", one commentator said. "You don't even see into them very far!" The missile tracks the laser beam. Once off the beam, there is no way it can get back on (a possible explanation for the impressive exercise in hedge-trimming). The chopper pilot knows (in something as sophisticated as the HIND) that he is being scanned, and has 30 seconds to do something about it, like dodge behind the nearest hill, which is a fairly effective protection against a line-of-sight system like ADATS. There is also the minor problem that the computer system can't tell friend from foe.

Reliability is a problem. Although the producers of the programme didn't seem to have a very clear idea of the difference between reliability, maintainability, and availability, a number of people made statements to the effect that the availability of the system is 40%. The system is thought to be so complex that its reliability may never reach an acceptable level. "Pilots are cautious people." remarked one interviewee. "If they find they're under attack from something like ADATS, they'll simply go away and come back when the system isn't working."

Why does this situation arise so often in modern weapons system development?

- There is a school of thought which believes that complex electronic systems are, or can be made, the answer to everything in modern warfare.
- Military careers are made on the backs of projects like ADATS. For those involved, there is no advantage in cancellation, even if it doesn't work.
 To get the troops something they can use is at most the third priority. (Senator Chuck Bernard).

Why is the US military persisting with ADATS?

As the senator said: "In this country, we seem to like turkeys!"

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Heads-up "Holograms" of Runways to assist in landings?

<rwood@vajra.pa.dec.com> Thu, 29 Nov 90 17:39:03 PST

Summarized from: {Business Week Nov 19, 1990}

Seattle's fog is legendary, but from now on it will not delay as many flights as it has in the past. Seattle-Tacoma International Airport is the first to win approval for takeoffs guided by new technology that lets a pilot see in thick fog. Developed by Flight Dynamics Inc., Portland OR, the system is similar to the heads-up display in jet fighters. A transparent screen flips down inside the windshield, and holographic images of the runway's center line and horizon are projected onto it. Thanks to special optical tricks, the images appear to be in front of the plane, where the real runway is. Alaska Airlines has been using the system for landings for the past year, but until now, the Federal Aviation Administration would not allow its use for takeoffs if visibility dropped below 600 feet.

Richard Wood Corporate Worksystems Team Digital Equipment Corp.

Airline safety

<sullivan@poincare.geom.umn.edu> Tue, 4 Dec 90 11:36:13 CST

This week's Economist has an article about airline safety, reminding us (as the Northwest crash yesterday did) that two-thirds of all accidents happen in the 5% of a flight around take-off and landing.

Although three-quarters of accidents are blamed on pilots' errors, pilots can be "set up" for an accident by many things, such as confusing instructions from air-traffic controllers or by picking the wrong switch in a badly designed cockpit.

The article focuses on four recommendations from Boeing for increased safety. None of them relates specifically to computer risks, though they all seem related to the safety and privacy concerns we have often discussed in RISKS.

1. Pilots should calculate before takeoff a "decision speed" at which takeoff can continue even with engine loss (rather than aborting and possibly going off the end of the runway). Such accidents are rare, but in 2/3 of the cases, the pilot is found later to have made the

wrong decision.

2. Install new Ground Proximity Warning Systems (GPWS):

Early GPWS systems can be unreliable and are prone to giving false alarms. ... this means they eventually get ignored--or disconnected. Pilots can easily turn them off in the cockpit.

3. Install more ILS (Instrument Landing Systems) at airports. This would encourage fewer "nonstabilised" approaches at high speed.

4. Make more use of flight-data recorder (black box) info, which could be "highly valuable for training". This "final suggestion is controversial" although already used by some airlines in Europe. The Economist closes:

[T]here is opposition from some pilots and their unions. They reckon that the recorders--which also make a tape of flight-deck conversations--could become a "spy" in the cockpit. Passengers might think that a good idea.

John Sullivan

As the spacecraft turn

<smb@ulysses.att.com> Wed, 05 Dec 90 11:09:41 EST

This doesn't appear to be a very good week for computers in space... I'll let others tell the myriad stories about what's going on with the space shuttle's telescopes, but a lot of the problems appear to be computer-related. For example, one attempt to fix some star tracker problems involved patching some software, because the tracker was more sensitive than thought. Unfortunately, the patch was loaded into the wrong computer.

On another (orbital) plane, Magellan lost several mapping orbits worth of data because of a data entry error. It seems that the commands downloaded (uploaded?) didn't have the required blank delimiters; consequently, the orbiter correctly rejected the entire sequence.

--Steve Bellovin

NeXT microphone problem?

"E. Loren Buhle, Jr. [215-662-3084]" <UHLE@xrt.upenn.edu> Tue, 27 Nov 90 12:56 EDT

THIS MESSAGE DEALS WITH A POSSIBLE "RISK" PERTAINING TO CONTROL OF THE INTEGRAL MICROPHONE IN THE LATEST NEXT MACHINE.

FIRST, SOME DESCRIPTION:

The newest NeXT machine has a microphone in the lower left portion of the CRT console (embedded in the plastic frame of the CRT). This integral microphone is an important input device for the voice annotation software running on the NeXT. It comes with all new NeXT machines. The software interface on the NeXT presents the user with keys corresponding to a tape recorder (e.g. record, stop, rewind, play, etc.). The user hits the record button, speaks for any length of time, hits stop, rewind, play and hears the conversation that was recorded to a disk file (and played back) very nice touch!

The operating system on the NeXT machine is Mach UNIX, a multiuser environment. NOTHING APPEARS TO PREVENT REMOTE OPERATION OF THE MICROPHONE. There is NO INDICATION ON THE FRONT OF THE NEXT MACHINE THAT THE MICROPHONE IS LIVE OR DEAD! (Remember Ronald Reagan's problems with "supposedly dead" microphones?)

Here is a scenario: A remote user turns on the microphone on the NeXT, recording the voice to a file (locally or remotely). Any sound in the proximity of the NeXT CRT is recorded. This file containing the conversation is then played back on a remote NeXT. Voila, a built-in office bug! While it can be argued that control of the microphone is by the console, anyone with superuser privs can undoubtable find a workaround.

On the old (1988 vintage) NeXT box, the microphone was plugged into a jack on the back. Unplugging the microphone removed this problem. Cumbersome, but very effective. The new microphone is built into the CRT case. It is not trivial to detach/attach at will.

So what can be done? One possibility would be to have a physical LED turn on whenever the microphone was active. This LED would be physically wired to the microphone and NOT be under program control. This possibility assumes the people carrying on the conversation are looking at the NeXT console...

Thoughts?

Dr. E. Loren Buhle, Jr. INTERNET: BUHLE@XRT.UPENN.EDU University of Pennsylvania School of Medicine Phone: 215-662-3084 Rm 440A, 3401 Walnut St., Philadelphia, PA 19104-6228 FAX: 215-349-5978

Risks of global networking

Hank Nussbacher <ANK@BARILVM.BITNET> Wed, 28 Nov 90 09:45:05 O

Over the past few months I have noticed upon occasion files that appear in our system that arrive from a fellow Bitnet system named NCCIBM1. The files always remain in the RSCS print queue since they are destined for the system printer. I always purged them, since there was never any indication that they were intended for any user on our system - BARILVM (Bar-Ilan University in Israel).

This past week I decided to track down the people at NCCIBM1 and find out why we are getting their job outputs. NCCIBM1 (USA Environmental Protection Agency in North Carolina) determined that their JES system has BARILVM listed as node #178. They also have a remote printer listed as #178. Rather than typing R178

for her output JCL, the user made a mistake and typed N178 - which sent the output to Israel rather to some printer in North Carolina.

Is this a risk of computer networking? I bet over the past year there has been a very irate user in North Carolina trying to find her job outputs. All she had to do was hop on a plane and fly a few thousand miles to find her MVS output. :-)

Hank Nussbacher, Computer Center, Bar Ilan University

Mook Review - Technological Risk by H. W. Lewis

Jake Livni <jake@bony1.bony.com> Wed, 28 Nov 90 21:39:35 EST

In the Sunday New York Times book review section (Nov. 25, 1990), there was a review of:

Technological Risk by H. W. Lewis 353 pp. New York W. W. Norton & Company. \$22.95

According to the reviewer, it seems to be an interesting and surprising view of risks in technology. The author, "a physicist at UCSB", shows that many technological risks are overshadowed by similar natural risks and that concern over technological disasters may be overdone.

I haven't seen this book, so I'm just notifying you about the article / review.

* ``Hackers Accessed NASA's Phones''

<[anonymous]> Thu, 6 Dec 1990

Today's AP wire, datelined HOUSTON, and reported in the Houston Chronicle, noted that computer intruders have stolen some \$12 million in free telephone service through Johnson Space Center... That figure was calculated from costs of similar break-ins described by law enforcement agents specializing in computer crime. A long-distance credit card number was used, as well as NASA's phone lines. The credit card fraud was discovered by AT&T when use of the number exceeded typical patterns. An earlier report, on 17 Nov 90, noted that phone service worth millions had been similarly obtained from the Houston offices of the Drug Enforcement Administration. Both cases involved intrusions to the Federal Telephone System, which apparently has little or no accountability.

Hacker view of the "Legion of Doom" sentencing in Atlanta

Emmanuel Goldstein <emmanuel@well.UUCP> Fri, 30 Nov 90 01:00:21 pst

The following is from the forthcoming Autumn 1990 edition of 2600, The Hacker Quarterly. We would appreciate it being distributed to as many interested people as possible. We consider this to be a very major and very frightening issue. If there are any questions or comments, we can be reached at 2600@well.sf.ca.us or (516) 751-2600.

Emmanuel Goldstein, Editor, 2600 Magazine

Over the past year there has been a great deal of publicity concerning the actions of computer hackers. Since we began publishing in 1984 we've pointed out cases of hackers being unfairly prosecuted and victimized. We wish we could say things were getting better but we cannot. Events of recent months have made it painfully clear that the authorities, above all else, want to "send a message". That message of course being that hacking is not good. And there seems to be no limit as to how far they will go to send that message.

And so we come to the latest chapter in this saga: the sentencing of three hackers in Atlanta, Georgia on November 16. The three, Robert Riggs (The Prophet), Frank Darden, Jr. (The Leftist), and Adam Grant (The Urville) were members of the Legion of Doom, one of the country's leading hacker "groups". Members of LOD were spread all over the world but there was no real organization, just a desire to learn and share information. Hardly a gang of terrorists, as the authorities set out to prove.

The three Atlanta hackers had pleaded guilty to various charges of hacking, particularly concerning SBDN (the Southern Bell Data Network, operated by BellSouth). Supposedly Riggs had accessed SBDN and sent the now famous 911 document to Craig Neidorf for publication in PHRACK. Earlier this year, BellSouth valued the document at nearly \$80,000. However, during Neidorf's trial, it was revealed that the document was really worth \$13. That was enough to convince the government to drop the case.

But Riggs, Darden, and Grant had already pleaded guilty to accessing BellSouth's computer. Even though the facts in the Neidorf case showed the world how absurd BellSouth's accusations were, the "Atlanta Three" were sentenced as if every word had been true. Which explains why each of them received substantial prison time, 21 months for Riggs, 14 months for the others. We're told they could have gotten even more.

This kind of a sentence sends a message all right. The message is that the legal system has no idea how to handle computer hacking. Here we have a case where some curious people logged into a phone company's computer system. No cases of damage to the system were ever attributed to them. They shared information which we now know was practically worthless. And they never profited in any way, except to gain knowledge. Yet they are being treated as if they were guilty of rape or manslaughter. Why is this?

In addition to going to prison, the three must pay \$233,000 in restitution. Again, it's a complete mystery as to how this staggering figure was arrived at. BellSouth claimed that approximate figure in "stolen logins/passwords" which we have a great deal of trouble understanding. Nobody can tell us exactly what that means. And there's more. BellSouth claims to have spent \$1.5 million tracking down these individuals. That's right, one and a half million dollars for the phone company to trace three people! And then they had to go and spend \$3 million in additional security. Perhaps if they had sprung for security in the first place, this would never have happened. But, of course, then they would have never gotten to send the message to all the hackers and potential hackers out there.

We think it's time concerned people sent a message of their own. Three young people are going to prison because a large company left its doors wide open and doesn't want to take any responsibility. That in itself is a criminal act.

We've always believed that if people cause damage or create a nuisance, they should pay the price. In fact, the LOD believed this too. So do most hackers. And so does the legal system. By blowing things way out of proportion because computers were involved, the government is telling us they really don't know what's going on or how to handle it. And that is a scary situation.

If the media had been on top of this story and had been able to grasp its meaning, things might have been very different indeed. And if BellSouth's gross exaggerations had been taken into account at the sentencing, this injustice couldn't have occurred. Consider this: if Riggs' sentence were as much of an exaggeration as BellSouth's stated value of their \$13 document, he would be able to serve it in full in just over two hours. And the \$233,000 in restitution would be under \$40. So how much damage are we really talking about? Don't look to BellSouth for answers.

In early 1991, the three are to begin their sentences. Before that happens, we need to reach as many people as possible with this message. We don't know if it will make a difference in this particular case if the general public, government officials, and the media hear this side of the story. But we do know it would be criminal not to try.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Marjory Blumenthal <BLUMENT@NAS.BITNET> Fri, 07 Dec 90 10:02:00 EDT

COMPUTERS AT RISK: Safe Computing in the Information Age National Research Council, System Security Study Committee

Computers play a crucial role in virtually every facet of modern life in the United States, from transportation safety to business and banking transactions to health care. Yet as computer systems become more prevalent, sophisticated and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and computer viruses and other attacks on computer systems. The result may be economic disaster, threats to human life, and compromise of confidential information held in computer databases. Increased use of computer networks, as well as a general rise in computer literacy, make it likely that the nation's computer security problems are just beginning. Computers at Risk, a new report from the Computer Science and Telecommunications Board of the National Research Council, presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The recommendations are fully developed and wide ranging, addressing the roles of specific agencies, expansion of current programs, cooperation between government and industry, and more. The volume outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. Computer system vulnerabilities are analyzed, and government security efforts are evaluated. Business executives, government security specialists, hardware and software developers, system managers, researchers, educators, and computer users will find this book vital to their understanding of computer security issues.

CONTENTS:

Executive Summary

Overview and Recommendations: Computer System Security Concerns, Trends, The Need to Respond, Toward a Planned Approach, Nature of Security, Putting the Need for Secrecy into Perspective, Building on Existing Foundations, Recommendations

Concepts of Information Security: Security Policies, Management Controls, Risks and Vulnerabilities, Securing the Whole System

Technology to Achieve Secure Computer Systems: Specification vs. Implementation, Models, Services, Trusted Computing Base, Communications

Programming Methodology: Programming Languages, Specifications, Formal Specification and Verification, Hazard Analysis, Development Process, Procurement, Scheduling, Education and Training, Management Concerns, What Makes Secure Software Different, Recommended Approaches

Criteria to Evaluate Computer and Network Security: Security Evaluation Criteria, Assurance Evaluation, Trade-offs in Grouping of Criteria, Comparing National Criteria Sets, Reciprocity, System Certification vs. Product Evaluation

Why the Security Market Has Not Worked Well: The Market for Trustworthy Systems, Concerns of Vendors, Federal Government Influence, Export Controls, Consumer Awareness, Regulation

The Need to Establish an Information Security Foundation: Attributes and Functions, Other Organizations, Charter and Startup Considerations, History of Government Involvement, Security Practitioners

Research Topics and Funding: A Proposed Agenda, Directions for Funding Security Research

Bibliography, Appendixes, Glossary

ISBN 0-309-04388-3; 1990, 320 pages, 6 x 9, paperbound, \$19.95

Please send me _____ copy(ies) of Computers at Risk: Safe Computing in the Information Age.

I have enclosed a c	check for \$ Please bill my
MasterCard	_ VISA American Express account.
#	Expires
Signature	Phone number
Name	
Address	
City	State Zip Code
	COUNTRY if not USA
Quantity Discounts	s: 5-24 copies 15%, 25+ copies 25%
3:30-5:00 EST. Call applies only in the [I have received	(202) 334-3313 in the Washington metropolitan area. Price U.S., Canada, and Mexico and may be changed without notice. so many requests for this information yesterday and today
🗡 Computers U	nder Attack
Patar Danning <ni< th=""><th>d@riggs adus</th></ni<>	d@riggs adus
Thu, 6 Dec 90 15:0	00:32 PST
COMPUTERS UNI	DER ATTACK
Intruders, Worm	is, and Viruses
Edited by Peter J	J. Denning
	nuuisoii-vuesiey, 1990, 334µµ mhars \$20.50 othars
οτο.ου acivi mer	mbers, 220.30 others
On behalf of ACM	Press and the authors of the 38 articles brought together in
this edition, I am p	proud to announce that our book on the subject of attacks on
computers is now	available.
This subject contin	nues to receive ongoing attention in the national proce
for example the m	ecent discovery of \$12M of tall fraud at the NASA Johnson
son example, the re Space Center One	eterni uistovery or \$1210 or ton indudid the NASA Johnson
broaking in to the	
report, "Computer	Rell System, and the recent splashy appearance of the NPC
	Bell System, and the recent splashy appearance of the NRC s at Risk".
The purpose of thi	Bell System, and the recent splashy appearance of the NRC rs at Risk".
The purpose of thi words of those wh	Bell System, and the recent splashy appearance of the NRC rs at Risk". is book is to tell the story of attacks on computers in the to are making the story and who see the broad perspective in
ne purpose of thi ords of those wh	Bell System, and the recent splashy appearance of the NRC rs at Risk". is book is to tell the story of attacks on computers in the to are making the story and who see the broad perspective in

provided connective material to bring out the global context and show that the problem is not purely technology, not purely people, but a product of the interaction between people and computers in a growing worldwide network.

After and introduction and preface by me, the articles are arranged in six parts. Most of these have been previously published, but there are a few new pieces specifically commissioned for this volume.

PART I: THE WORLDWIDE NETWORK OF COMPUTERS

Worldnet and ARPANET by Denning, overview of networks by Quarterman, reflections by Thompson, survey of computer insecurities by Witten.

PART II: INTRUDERS

Reflections by Reid, Wily hacker story by Stoll, a followup commentary by Mandel, and a business perspective by Wilkes.

PART III: WORMS

Internet worm overview by Denning, perspectives on the Morris worm by MIT's Rochlis et al, Purdue's Spafford, and Utah's Seeley, executive summary of Cornell Report, Morris indictment and trial summary by Montz, original worm paper by Shoch and Hupp.

PART IV: VIRUSES

Virus overview by Denning, BRAIN and other virus operation by Highland, virus primer by Spafford et al, viral protection in MS/DOS by Brothers, and a perspective on viruses by Cohen.

PART V: COUNTERCULTURES

Computer property rights by Stallman, cyberspace literature by Paul Saffo, a dialog on hacking and security by Dorothy Denning and Frank Drake.

PART VI: SOCIAL, LEGAL, AND ETHICAL IMPLICATIONS

A spectrum of commentaries: moral clarity and sending a signal by Denning, global city by Morris, virus bills in congress by Crawford, GAO report summary, legal issues by Samuelson and by Gemingani, computer emergency response by Scherlis et al, ethics statements by various organizations, ACM President's letters by Kocher, ACM forum letters, law and order for the PC by Director, RISKS perspectives by Neumann, crimoids by Parker.

To order the book, run to your local bookstore or call ACM Press Order Department. For credit card orders only call 800-342-6626 or in Maryland and outside the continental US call 301-528-4261 and for mail orders ACM Order Department, P. O. Box 64145, Baltimore, MD 21264. The price for ACM members is \$18.50 and for nonmembers \$20.50. Shipping is extra unless you send a check to the order department. BE SURE TO INCLUDE YOUR ACM MEMBER NUMBER AND THE BOOK ORDER NUMBER (706900).

* ``Hackers Accessed NASA's Phones'' (Re: <u>RISKS-10.65</u>)

The Polymath <hollombe@ttidca.tti.com> 7 Dec 90 17:23:55 GMT

According to yesterday's news NASA has flatly denied the theft ever took place. Their spokesperson said their normal annual phone bill is about \$3 million and it wasn't possible for someone to steal \$12 million worth of phone services from them (i.e.: They'd be detected long before things got that far out of hand).

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

Kesponse to article on "Legion of Doom" sentencing (<u>RISKS-10.65</u>)

&ary_Cattarin@dg_support.ceo> Fri, 7 Dec 90 10:42:30 est

CEO document contents<:

The article that appeared in <u>risks 10.65</u> from Emmanuel Goldstein of "2600" Magazine displays a callous immaturity to the realities of the business world. I'm not going to quibble over the exact nature of the sentences handed out. The clear point, and yes, the "message" that the authorities tried to get across (but was clearly lost on the author of that article) is that unauthorized access to someone else's computer is just plain wrong, no matter what was or was not done during that access.

We've heard that point reiterated numerous times in this journal, and I'm sure the hackers of the world have heard it and usually discounted it, but let me put it in the vein of the realities of modern business.

Mr. Goldstein, I don't know a thing about your magazine. I don't know your organization's finances, staffing, etcetera, or if you even have any of them. I don't know what you do for a living. I do know that in my business, we are faced with an intensely competetive global marketplace in which we fight to survive. We are faced with the realities of staff shortages compounded by further cuts. We are faced with shortages of resources, yet we still must get the job, or it will mean the end of our jobs, and probably the end of the company as well.

We would LOVE to have enough time to do everything perfect. We'd LOVE to devise security systems that could foil you and your clan. And we could probably come pretty damn near doing it; we've got some pretty good heads here - most likely some heads who have done their share of hacking as well. But we can't dedicate that kind of time to staving off a bunch of obnoxious intruders, just as Bell South didn't. Bell South dedicated their personel to doing the business they were involved in, as rightly they should.

So what happens when you invade Bell South's, or my company's computer? If you get in, just to prove you can, then tell us about it

in light of your supposed "spirit of pointing out flaws that should be fixed", what has that gained you? Giddy joy, I suppose, but not much else (picture the job interview: "So, what are our technical qualifications?" "Well, sir, I'm good. I broke into 43 systems last year!"). What has it gained us? OK, we know about a flaw. You know what? We probably already did. Perhaps you don't realize it, but in the resource-short business world, we know about a LOT of flaws. We'd LOVE to fix them all. We're trying. We just don't have the resources to get it done immediately.

So that leaves the door that you found. Now you'll spread word of your door via your hacker hotlines. And though you may have meant no harm, others may follow, invading our system as if it were another town on the interstate to be driven through.

But can you or we be sure that all who enter mean no harm? Can you be sure that no bit was left untouched? That's all it takes: one bit, somewhere, modified, which, as readers of RISKS well know, can have monumental consequences. The downing of an airliner. A fatal safety flaw in a new car. An accounting system rendered worthless. These are major cases, but the minor ones are just as important, because once you've been invaded, you just don't know what the invader did.

If you came home at night and found your front door unlocked, what do you know? Sure, you may have left it unlocked. But did anyone take advantage of that? Did they take anything? Damage anything? Leave anything unwanted inside? Steal the extra key? Are they perhaps even in your home?

Didn't you check to be sure that door was locked? Maybe you did, but they came in through the window. Didn't damage anything, but still, you don't know that? OK, you checked the windows, but they came in through the skylight. You checked those? They found another way...

You see, you can take care of all the obvious points of entry, but a intruder will find another point of entry. The hacker's view is that since that other point of entry wasn't blocked off, the hacker is welcome in. I don't think you'd agree if it were your home.

So Bell South detected an intruder. And they chose to pursue the intrusion. How much did it cost them? Was it simply the "value" of the document? (How does one place a value on a document?) Was it simply the cost of the personel who investigated? Was it perhaps the business lost because they spent their time looking for the intruder instead of pursuing Bell South's normal business? (Remember, Bell South is in business to make money, like it or not. Your nation is build on that principle, that's why you can get food in your grocery store, unlike in Moscow.) Was it the cost of implementing modified procedures company-wide to protect against the likes of you? The cost of business lost because people company-wide spent time on these new procedures rather than pursuing their intended business? How about the cost (real and lost opportunity) of the personnel involved in the legal case, not to mention the lawyers' fees? You see, "cost" has a much more far reaching meaning than you attribute to it. And nobody

can really even tell how high the final figure is, but I'll assure you, it's astronomical.

In business, we've got to spend our time and resources pursuing our business. We just don't have the time, money, or resources to post guards to keep the likes of you out of every possible entry point. Until you understand that, the government is going to continue to try to send you this message. Perhaps my treatise here will save you and your colleagues a few prison terms (pity the fact that I, as a taxpayer, have to support those folks in prison!). More importantly, perhaps it will spare a few other companies the trouble that Bell South has experienced.

Kesponse to article on "Legion of Doom" sentencing (<u>RISKS-10.65</u>)

King Ables <ables@mcc.com> Fri, 7 Dec 90 10:28:22 CST

I read your article on the sentencing of some "Legion of Doom" members that was posted to comp.risks and feel compelled to make a couple of remarks.

I agree that this situation is one about which we, as a community of programmers, should be concerned. But the tone of panic seems meant to persuade us emotionally rather than intellectually.

> This kind of a sentence sends a message all right. The message is that the> legal system has no idea how to handle computer hacking.

This, unfortunately, is very true. It is also the main reason we have the problems you describe. If the laws were written better (i.e. the issues involved were better understood by those who write the laws) many of these problems wouldn't exist.

> shared information which we now know was practically worthless. And they
 > never profited in any way, except to gain knowledge. Yet they are being
 > treated as if they were guilty of rape or manslaughter. Why is this?

Whether or not you profit from something has nothing to do with whether or not it was a crime. You don't profit from beating the hell out of some homeless person in an alley, but it's still illegal.

They are being treated like criminals because they participated in a criminal act. If you don't believe the activity should be considered illegal, then work to get the laws changed. Right now-- today-- at this moment-- the acts are illegal. Whether or not they SHOULD be illegal is a completely separate question.

> We think it's time concerned people sent a message of their own. Three young
 > people are going to prison because a large company left its doors wide open
 > and doesn't want to take any responsibility. That in itself is a criminal act.

Nope. Three young people are going to prison because they broke the law.

If I walk into an unlocked jewelry store and take something, it is no less a crime. To say that the establishment deserved it because they left themselves wide open for it is hardly a justification for the action.

> By blowing things way out of proportion because
> computers were involved, the government is telling us they really don't know
> what's going on or how to handle it. And that is a scary situation.

This is absolutely true. And again, by participating and contributing our knowledge to the process, we can help to modify the process so that it makes more sense. To simply sit back and scream "foul" isn't going to make it any better.

This is not to say I believe the accused received appropriate punishment, I don't. But to claim they are innocent victims of the big, bad government is not correct either.

King Ables, Micro Electronics and Computer Technology Corp., 3500 W. Balcones Center Drive Austin, TX 78759 +1 512 338 3749

Kesponse to article on "Legion of Doom" sentencing (<u>RISKS-10.65</u>)

Brinton Cooper <abc@BRL.MIL> Fri, 7 Dec 90 13:39:23 EST

Emmanuel Goldstein, Editor, 2600 Magazine, quotes from his pub:

"...We consider this to be a very major and very frightening issue... Since we began publishing in 1984 we've pointed out cases of hackers being unfairly prosecuted and victimized...just a desire to learn and share information... Here we have a case where some curious people logged into a phone company's computer system...No cases of damage to the system were ever attributed to them...We think it's time concerned people sent a message of their own. Three young people are going to prison because a large company left its doors wide open and doesn't want to take any responsibility. That in itself is a criminal act..."

1. Leaving one's doors open is not a criminal act. When was was anyone ever prosecuted for failing to lock the garage door?

2. Breaking and entering is a crime in most jurisdictions. Sentences of 14 to 21 months don't sound uncommon for breaking and entering.

3. The general public has no inherent right to "information" owned by a phone company, any other company, or private individuals, except as prescribed by law...and even then, not always. Breaking and entering someone's home in order to listen to their stereo, read from their library, or peruse their family's financial files is no one's right.

_BRINT

Response to article on "Legion of Doom" sentencing (<u>RISKS-10.65</u>)

Mark E. Levy <levy%fndcd.dnet@fngate> Fri, 7 Dec 90 15:43:54 CST

Emmanuel Goldstein, Editor, 2600 Magazine writes:

>... We think it's time concerned people sent a message of their own. Three young >people are going to prison because a large company left its doors wide open and >doesn't want to take any responsibility. That in itself is a criminal act. ...

Sorry. I don't buy it. If I leave my keys in my car with the windows open, and you get in and drive off, you're still just as guilty of stealing the car as if you had to break in and "hot wire" it. I may have asked for it by leaving the keys, but that's no excuse.

By the same token, you have no implied right to come into my house and "look around" just because I left the door open. It's no different with computers. Irrespective of whether of not BellSouth "left the door open," if the three you mentioned entered the system without permission, they're guilty. That in itself is enought to convict, any materials taken nonwithstanding. Case closed. I have NO sympathy for them.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



🗡 Airline safety

Donald A Norman-UCSD Cog Sci Dept <danorman@UCSD.EDU> Fri, 7 Dec 90 08:00:20 PST

I apologize in advance: this is a sermon.

The note in RISKS on the Economist's suggestions for aviation safety prompts this note. The problem is that the suggestions were all aimed at the pilots. The myth of crashes caused by single individuals, usually the pilot, persists.

Accidents in aviation is a system problem. Accidents occur because the system is faulty. Note that an accident almost never involves a single error: there must be a chain of events, each of them usually unlikely by themselves, before an accident happens.

The Economist's suggestions seem to me to be without merit, save for their last -- that we should get more information from the cockpit. I was pleased and

surprised to see the NTSB (the U.S. National Transportation Safety Board) just recommend increasing the voice cockpit recorder tape to longer than 30 minutes (now it is a repeating loop of tape of duration 30 minutes), increasing the number of parameters measured by the black box that records airplane and engine state, and hurrah! adding video cameras and recorders so you could see if critical controls were actually used.

Accidents will continue as long as people treat this as something that can be cured by concentration on the pilots. In my opinion, the flight-deck instrumentation -- especially the automation, such as the "flight management computer" and "mode control panels" are classic examples of poor design from the human side of things, the maps and approach charts are unbelievably cluttered and complex (a recent accident in which a landing aircraft clipped the power lines, thus turning off the airport's landing lights (among other things) was partially attributed to incorrect reading of the charts), and the interactions with air traffic control (ATC) and the equipment and limitations that ATC face add to the problem.

The new addition of "datalink" to the cockpit will only create new problems. Datalink is digital transmission of ATC information to be received somewhere in the cockpit on a CRT display. This replaces some of the voice communication on the now overcrowded channels. In principle it has merits, but it is yet another complex piece of equipment, yet another change in procedures, yet another bandaid and ill-considered addition to cockpit clutter. I used the word "somewhere" because nobody yet knows quite where to fit the thing into the already crowded cockpit, and all the current suggestions seem to lead to foreseeable future problems. The lack of positive confirmation form pilots will also lead to other (foreseeable) problems. Basically, one cannot fix a system problem by adding local patches. In fact, that tends to make things worse.

These difficulties have been known for a long time. The only surprise about the recent runway collision in Detroit (where a plane taxiing on the runway collided with a plane taking off on the same runway) is that it hasn't happened frequently before. The NTSB had warned about these problems. Pilots know they get lost on runways and taxiways, and the Tenerife crash that destroyed two fully-loaded 747's some years ago was almost identical. It is a system problem.

As long as we try to solve the problem by arguing that pilots need better decision rules or better warning systems, then we are going to continue to have the problem.

Human error is almost always a result of system or design error, and unless you attack that, you don't attack the causes.

The Economist urged the introduction of a new decision speed. Sigh. Loss of an engine on takeoff is what every pilot practices and what almost never happens, and the current decision speed of V1 should probably be degraded, but it is NOT the main culprit. The Economist said that the current ground proximity warning systems (GPWS) are faulty. The last thing a pilot needs is yet another warning system in the cockpit. And I don't recall any recent incidents where a faulty GPWS was a contributors. By the way, substitute "computer" or "ship or "oil refinery" or "chemical plant" for "airplane" and substitute "operator" for "pilot" and you get the same message. Society tends to try to find single individuals to blame for accidents. Students of human error blame the system. And unless we fix the system, we will continue to have these accidents as a mater of course. "Normal accidents" is what Charles Perrow called them in his brilliant book by that title.

Credentials: I study aviation safety under a grant from NASA. No, I am not a pilot.

Don Norman, Department of Cognitive Science 0515, University of California, San Diego La Jolla, California 92093 USA BITNET: dnorman@ucsd

Voter identity and Dial-A-Vote

Lauren Weinstein <lauren@vortex.com> Wed, 21 Nov 90 22:55:20 PST

One risk that I don't think I saw mentioned in the discussion of "Dial-A-Vote" systems relates to the identity of voters. Such a system, by definition, would need to know the identity of each caller to check registration and avoid duplications. Caller-ID would require people's presence at particular phones and is a can of worms for many other reasons. Personal ID codes could also be used, but, uh, I *wonder* what number would be most likely used for this purpose? Can you say "SS"? I knew you could!

In any case, you'd have to identify yourself to the system, and then it would be trivial for a file to be kept on how you voted. Of course, we'd be told that this wouldn't be done, that there would be adequate safeguards, and that it was *impossible* to subvert the system.

This is a significant new risk. With current voting techniques, picking out an individual's vote is essentially impossible without a great deal of illicit goings on at the polling place. Paper ballots and punch card ballots have no identifications, and are thrown into common bins. Voting machines increment internal counters that keep running totals only, not individual votes. But with Dial-A-Vote, all this low-tech privacy goes out the proverbial window.

--Lauren--

Voting electronically from home

Glen Overby <overby@plains.NoDak.edu> Sun, 25 Nov 90 02:01:47 -0600

I have a few items to contribute to the vote-by-phone discussion. First, how do you identify legitimate voters? While most states require voters to register before an election, North Dakota does not, and I don't believe we're alone in that aspect. In fact, I have never been asked to show any type of identification; I am merely asked my name and address (the first time I voted I

was asked to sign a form stating that I was using my real name, of voting age, had not voted in another precinct, etc.). Telephone voting could be possible if you have voted in a previous election, and are thus in your precinct's records. This does not permit a complete transition over to automated voting, but could allow it's addition as a convenience.

You will, nonetheless, have to identify yourself on the telephone with some sort of number. There will have to be laws passed insuring your privacy as well as illegitimate use of someone else's voter-id number; imagine how some phreak with an autodialer could wreak havoc with an election by voting "for" people.

The other thing missing from the vote-by-phone system is the provision for write-in candidates. I'm not certain if all states require a provision for write-in candidates, but many years ago the mechanical voting machines here were replaced with fill-in-the-dot forms that are optically scanned by a couple of IBM scanners down at the courthouse. I recall the issue of the switchover was not one of mechanical reliability (those machines were OLD), but that there was no way for you to write-in a candidate.

Glen Overby <overby@plains.nodak.edu> uunet!plains!overby (UUCP) overby@plains (Bitnet)

Voting from home electronically

Paul Peters <Peters@DOCKMASTER.NCSC.MIL> Mon, 26 Nov 90 08:43 EST

The emphasis of <u>RISKS 10.64</u> on telephonic voting taking rights away from the population without telephones is misplaced. Of all the problems with telephonic voting, this is the least. One could say that the current locations of polling places takes rights away from those without automobiles, but we have found ways to provide alternate transportation for those folks. With some creativity, we could find ways to provide voting capability to those without telephones also. Paul Peters

remote voting: the Oregon experience

Andrew Klossner <andrew@frip.wv.tek.com> Thu, 29 Nov 90 10:59:07 PST

Experience in Oregon with remote voting may shed some light on proposals for vote-by-telephone. Oregon has used vote-by-mail for special elections for a few years.

A few weeks before the election, each registered voter receives, by mail, a perforated punch card and explanatory material. To vote, we punch the card appropriately (using a pencil to poke out perforated holes), seal the card in a special envelope, sign the envelope, and mail it. We have to pay for the stamp. Only one ballot per envelope. During such elections, the usual polling places are not established. Anybody who objects to vote-by-mail must go to the county seat on election day to vote in person. Not only is this a potential hardship, but so few people do this that they lose the anonymity of large numbers.

This system is subject to many of the potential pitfalls mentioned by other contributors. Perhaps the greatest of these is that the dominant member of the household can punch all the cards, coerce signatures from other members, and thus influence several votes. Another is that we, the electorate, have no guarantee of ballot secrecy other than the solemn promise of the bureacracy.

Reported public opinion is unanimously in favor of vote-by-mail because it reduces the cost of an election (no polling place expenses) and because we get much greater voter participation.

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

Re: Voting (Re: <u>RISKS-10.61</u>)

Dan Sandin <sandin@uicbert.eecs.uic.edu> Thu, 29 Nov 90 22:45:46 GMT

OK, my response to what has gone down so far:

making election day a national holiday, or whatever, still would not make it better for every person to get to the polls. I mean, think about all the people who still have to work on national holidays, or even have to work MORE (liquor store employees spring immediately to mind) or cases when unforeseen circumstances prevent one from voting. A sick sister in another state, a boiler explodes, whatever.

The point is simply to make legitimate voting EASIER.

As we know from working with computers, plenty of people would prefer to vote the old-fashioned way, physically showing up at the polls, who don't trust, don't understand, or just don't like the phone-in system, that's just fine.

Someone suggested it would make blackmail voting, etc, easier. Remember, though, that usually "stealing" one vote, or even a thousand votes will make very little difference (depending on the size of the election) Ordering hundreds of little old ladies to vote by gunpoint would be very difficult to hide, and would only make a difference in a very small election. It is much safer and cost-effective to use the tried and true method of getting votes - getting the voters drunk.

Indeed, with this system, I would think that the regular polling places would just be custom terminals with leased lines direct to the same polling computer that one dials in with from home.

I would hope that one of the effects would be to encourage more voting, and perhaps for our government to have regular referenda on issues, rather than waiting for regularly scheduled elections. Just dial 1-800-PRO-CHOI or 1-800-PRO_ABRT

Some posters have suggested that a segment of the population would be favoured by this, that poor people would find it harder to vote than rich. True. However, I think you will find that the percentage of people who have telephones is greater than the percentage of registered voters who vote, let alone the percentage of the population as a whole who vote. I would guess that telephone market penetration is over 90%, and I would further guess that, considering payphones, work phones, a friend's phone, etc, >99.999 % of the population has phone access. In fact, since voter registration requires an address, I bet more people have access to phones than have legal residence addresses.

I think it is safe to say that if voting could be accomplished by phone as well as in a polling place, voting attendance would go up. And by definition with the tenets of Democracy, this is a Good Thing.

stephan meyers c/o dan sandin sandin@uicbert.eecs.uic.edu

p.s. someone mentioned the problem of tying up the phone lines, as in"I'm sorry, all voting lines are busy now, please try again later"This is a real problem, and probably no cheap way out of it.

Re: Voting (Re: <u>RISKS-10.61</u>)

Frank Kuiper <frankk@cwi.nl> 30 Nov 90 11:15:16 GMT

In the Netherlands we have the following system, wich works quite well. Everyone has a residents registration, no matter where in the Netherelands you live. This registeres, amongst other things, your name, address, date and place of birth.

With this information the councel (gemeente) knows who are eligible to vote. Every voter, some weeks before an election, is send a voting-card, with details on when and where (which polling station) to vote. The polling stations are open from 7am until 7pm (always on a Wednesday; no disturbance of the "Sunday peace" ;-), thereby giving everyone the opportunity to vote before, during or after work. It is possible to vote in another polling station, if you declare to want that. You will have to do that well in advance. Also, it is possible to have someone else vote for you, in which case you can easily transfer the received voting-card to the other voter, by mentiong his/her name on the card, and signing it yourself. One can only vote for two others (thereby making it very difficult to just buy all the voting cards).

Unless you're out of the country, have no friends or relatives and are dying somewhere, you always have the opportunity to have your vote cast. Residents outside the Netherlands can vote (by mail) via the local Dutch embassy.

All I have to do is pass the polling station on my way to work, and vote.

Frank Kuiper AppleLink: HOL0042

Ke: Becoming over-sensitive to risks (vote by phone)

Adams Douglas <adamsd@crash.cts.com> Wed Nov 21 22:57:14 1990

I was thinking about phone voting systems myself this last election. Specifically, I thought about the idea of having a centralized polling system which would allow you to enter your vote preferences during the campaign. This information could be used as official pre-election polls are used now. On election day, you would either call again and re-vote, or you could have specified earlier that if you did not call on election day, the system should use your last poll as your vote. This would solve a lot of absentee delays (and I know people will say there are problems with it, but it's just an idea).

"Little pitchers have big ears": yet another ATM RISK

<zowie@banneker.Stanford.EDU> Sun, 25 Nov 90 00:32:54 PST

Today, I went with a friend into a local bank [Wells Fargo], to activate his (newly-arrived) ATM card. This ritual involves the selection of a password [PIN] for for the account. He gave his card to the clerk, who swiped it through a magnetic reader and typed something on a keyboard. Then my friend typed his new PIN on a special, hooded keyboard out of view of the clerk (and, hopefully, from other bank clients).

A speaker clicked on, and, to my surprise, we (me; my friend; the clerk; and, in fact, nearly everyone in the building) were treated to the sounds of a dial tone, some touch-tone dial sounds, a (surprise!) normal-sounding 300-baud modem query and connection, and, in fact, the entire [300-baud] exchange, complete with hangup sounds.

The RISKS of this audible broadcast should be clear: anyone with a good pocket microcassette recorder should be able to record the entire modem transaction, simply by being near someone who is activating his ATM card. With a little ingenuity (or, eg, a DSP such as that onboard a NeXT machine), it would be trivial to decode the entire 'dialogue', which presumably includes not only the person's account number and PIN, but also a password to make changes to an arbitrary ATM card!

The information would be particularly easy to extract because of the robust nature of the 300-baud Bell standard.

I spoke with several colleagues (including joe@hanauma.stanford.edu) about the broadcast of the computer dialogue: it appears that many Wells Fargo branches follow this practice, and have been for at least three years.

The moral of the story is perhaps that one should not shout out sensitive information, even in supposedly unintelligible languages.

--zowie

Mailing software wastes money

<prm@ecn.purdue.edu> Wed, 28 Nov 90 10:13:41 EST

Last year my wife and I bought a chair at Michael's Furniture, a store here in West Lafayette. We financed the chair, and Michael's promptly sold the contract to Security Pacific Financial Corporation.

Everything went fine; no problems.

A month ago, we made our regular monthy payment, after which, our balance was some small amount (like 20 or 30 dollars). A week after we mailed our original payment my wife suggested that we just pay off the acocunt. I agreed. She wrote out a check for the balance due and mailed it off.

Fine, no problem.

A week ago, we got a bill from Security Pacific. For four cents. Apparently, some interest and accrued on the account in the week or so between checks.

Clearly, it never occured to the people writing Security Pacific's billing software that if the balance due was less than the cost of mailing a bill then they should just write off the balance due.

Sigh. We mailed them their four cents.

Phil



Search RISKS using swish-e

Report problems with the web pages to the maintainer



* Recent RISKS Mail to CSL.SRI.COM

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 13 Dec 1990 15:52:40 PST

Well, we survived the move to another building (I'm now in EL-243), although for a variety of reasons the servers could not be moved on schedule and getting everything working again was decidedly nontrivial. But the resulting outage of five days meant that some mail to CSL.SRI.COM was rejected. So, if you got BARFmail indicating your mail to CSL was undeliverable, PLEASE TRY AGAIN NOW. Sorry for the inconvenience. Peter

Many Bills Are Found Incorrect on Adjustable Rate Mortgages

Saul Tannenbaum <AUL_SY@hnrc.tufts.edu> Wed, 12 Dec 90 19:30 EDT

The New York Times reports (13 Dec 90) that, according to a General Accounting Office study, as many as 25% of all adjustable rate mortgage bills may be incorrect as a result of bank errors in calculating their interest rates. These error were found as part of routine audits done as failed savings and loan institutions were taken over by Federal regulators.

A former Federal mortgage banking auditor says that that estimate is too low, putting the problem at 30-35% of adjustable rate mortgages. In some cases, this auditor says, the errors resulted from "human mistakes" at small S&Ls, that often calculated adjustable mortgages by hand. In other cases the problems were caused by "computer glitches." One failed S&L, the Victor Federal Savings and Loan of Muskogee, Okla, was audited by the Bennington Group for the Federal Saving and Loan Insurance Corp. The audit, which sampled 96 adjustable mortgages, found that the bank's computer system contained logic error. The bank, among other things, rounded rates upward, instead of downward and "pulled" the index on the wrong date, when it might be higher or lower than on the correct date. Other errors resulted from "poor recordkeeping", where the indices on which the adjustable rates wer based couldn't be found, or did not match the FSLIC computer programs [which begs an obvious question]. Some adjustable mortgages have never been adjusted.

In one example given, a woman took out 3 identical adjustable rate mortgages from the same bank at the same time. Now, all three have wandered off in different directions. She has 3 different monthly payments, 3 different balances, and 2 payment schedules.

According to the article, it is the opinion of Federal regulators that the Truth In Lending Law "probably does not" require lenders to repay overcharges in any form.

Saul Tannenbaum, USDA Human Nutrition Research Center on Aging at Tufts University, 711 Washington St., Boston, MA 02111 STANNENB@TUFTS.BITNET

A White Xmas?

Brian Randell &rian.Randell@newcastle.ac.uk> Tue, 11 Dec 90 16:38:05 GMT

Date: Tue, 11 Dec 90 11:03:24 GMT >From: Rob Thirlby &.Thirlby@uk.ac.lut> Subject: Loughborough To: uk-mail-managers @ uk.ac.newcastle

We are back in the world, the little, forgotten, black hole in the East Midlands is now up and running after over 60 hours of no electricity, often no water, dodgy phones, and just to finish it off this morning a suspected gas leak and a heating fault (or at least I presume its a fault its not very warm!). Many of the surrounding villages are still without power and in some cases water and phones. And all this in the Soar valley with one of the lowest average snowfalls in England! The University cedar tree which features on much of our publicity has lost its top half and I suspect there has been more arborial damage than in the hurricane year.

For the technically minded the main problem was due to the incredibly wet sudden snowfall which stuck to anything it touched even in a gale. The Loughborough 132KV grid feed wires and gear fell onto a host of lower voltage feeders causing massive damage to both. It must have made firework night look tame. All our water is pumped by (non backed-up) electric pumps from Derbyshire and hence the chaos. There's nothing more irritating than being told on the radio to boil all the water when you havent any means of heating it. Mind you we can see the plumes of vapour from some of the countries largest power stations on the Trent and that doesnt improve ones temper when trying to bake potatoes on a log effect, real-flame, gas fire!

I hope you all had a nice week-end.

Rob Thirlby, Postmaster@lut

✓ Gender and computer anxiety

Rob Gross <<ROSS@BCVMS.BITNET<> Sat, 8 Dec 90 00:22 EST

The following is excerpted from the "Faculty File" column in the Princeton Alumni Weekly of December 5, 1990:

In general, [Joel] Cooper [chairman of the psychology department at Princeton] has found, females are more subject to computer anxiety than males are, and as a result, they perform computer-related tasks worse. But there's an important contextual component to these findings: the performance differential appears only when there's someone else in the room with the female who's using the computer. Just the presence of another person-male or female, no matter what he or she is doing-seems to be enough to generate computer anxiety. By contrast, when they're alone in a room with a computer, females generally show no appreciable difference in performance compared to males.

In the course of this study, Cooper examined a group of middle-school children in Princeton...The children were asked to solve arithmetic problems on a computer. In group settings, the girls in the class often did worse than the boys, whose performance actually improved when other people were around. In a test of university students, Cooper had groups of men and women play an adventure game called Zork on a computer; some played with other people present, other were alone. The middle school results were replicated. "We tried to get a fix on what the other people in the room had to do to provoke the computer anxiety," Cooper recalls. "It turned out to be almost nothing. They could be writing a letter in the corner, totally ignoring the woman at the keyboard, but still her performance would drop. They just had to be there."

Rob Gross Department of Mathematics BITNET: GROSS@BCVMS Boston College Internet: GROSS%BCVMS.BITNET@MITVMA.MIT.EDU Chestnut Hill, MA 02167

Computerized USA Phone Directory

Allan Meers - Sun Education <allans@ebay.sun.com> Thu, 13 Dec 90 00:03:32 PST

Mercury News - 90-Dec-12

Compuserve has introduced the FIRST computerized national phone book, listing the name, address, ZIP, and phone number of 80 million households in the US who have a listed number. As of December 1, the Phonefile service allows the 725,000 Compuserve subscribers to search the phone lists of the USA by:

name & address - for updating your christmas card list or for telemarketing reasons. This is just a computerized version of the current phone book - but without needing hundreds of phone books for the whole USA.

name & state - to find long-lost relatives or to find someone who has relocated (out of state). Examples include old classmates for class reunions, and birth parents of adoptees.

phone number - like a "reverse" directory, where you can get any listed name & address just by looking up the phone number.

The cost of retrieving the information is 25 cents per minute in addition to Compuserve's standard on-line charge of \$12.80 per hour (21 cents per minute). The cost is considered not much more than a call to directory assistance, and can be even cheaper considering the aquiring and search costs of all the phone books for the USA.

The Phonefile database is compiled by a direct marketing company, Metro Mail Corp. of Illinois, from phone directories, computerized real estate transactions, and other sources. It was not speculated on what the "other" sources might be, but I would suspect other telemarketing databases, magazine subscriptions, credit services, Usenet email alias lists :^}), and other public sources of name/address information. A Bellcore New Jersey privacy issues expert, James E. Katz, indicated that a likely consequence of the directory will be an even greater increase in the number of unlisted phone numbers in the United States. It was noted that Japan and European countries have practically no unlisted numbers, while the United States runs about 25% of its phone number unlisted, with 33% of California numbers unlisted.

While Compuserve assures that the directory was designed to discourage the compilation of marketing lists for junk mail and telemarketing, privacy experts assume that such use is inevitable. A magazine for instance, could compile phone numbers for a telemarketing campaign targeted at reader's whose subscriptions have lapsed.

✓ Getting out of Lotus' "Household Marketplace"

<todd@atd.dec.com> Wed, 12 Dec 90 09:44:29 -0800

If you don't want to be listed in the "Household Marketplace" database but you don't have enough energy to write a letter, you can also do the following:

Dial 1-800-343-5414 press 3, then 2 (I don't know what to do if you don't have a touch-tone phone.)

This will get you a human who will want to send you information about "Household Marketplace." However, you can also say that you want to be removed from the database. You will then be given the choice of mailing to Lotus or you can tell them your name and address and they say they will remove you from the database and send you written confirmation. I did this yesterday, so I know they will take your name and address. I can't vouch that they send the confirmation, the U.S. Mail isn't that fast.

If you are energetically opposed to this product, here are some names and addresses you might want to have for your own database:

Lotus Development Corp. 55 Cambridge Pkwy. Cambridge, MA 02142 (Mary Ann Malloy Coffey, Marketing Programs Manager) (Jim P. Manzi, Chairman, President, and CEO)

Equifax, Inc. 1600 Peachtree St. N.W. Atlanta, GA 30309 (Jeff V. White, Chairman of the Board) (C.B. Rogers, Jr., President and CEO)

Equifax is the original collector of the data which Lotus is selling. /tdn

🗡 update on Lotus

<todd@atd.dec.com> Wed, 12 Dec 90 13:54:14 -0800

Someone told me that they phoned Lotus today about getting off the Marketplace Household database and were told something different than I was told yesterday. Apparently, today's story is that if you want written confirmation that you've been removed from the database, you have to send mail to:

Lotus Development Corp. Attn: Marketplace Name Removal 55 Cambridge Pkwy. Cambridge, MA 02142

If you just phone them, they now say they won't send written confirmation. I wonder what they'll say tomorrow. /tdn

Ke: a fondness for turkeys (Re: Mellor, <u>RISKS-10.65</u>)

99700000 <haynes@ucscc.UCSC.EDU> Fri, 7 Dec 90 23:30:41 -0800

I'll suggest a third reason [for the problems Pete Mellor discussed in modern weapons system development], that I like to call Model Railroading. Designing a complex electronic system to solve some warfare problem is interesting, challenging, and fun; and somebody else is paying the bills. As long as we're not in a war, as long as the system doesn't have to solve some real problem, it is a delightful toy; and as with a model railroad we get to keep arranging the scenery so it appears to be doing the Real Thing.

✓ Call for Papers - 14th National Computer Security Conference

Jack Holleran &olleran@DOCKMASTER.NCSC.MIL> Sat, 8 Dec 90 23:32 EST

CALL FOR PAPERS 14th NATIONAL COMPUTER SECURITY CONFERENCE Sponsors: National Computer Security Center and National Institute of Standards and Technology

Theme: Information Systems Security: Requirements & Practices

OCTOBER 1-4, 1991 OMNI SHOREHAM HOTEL WASHINGTON, D.C.

The focus of the 14th NCS Conference will be on the "Experiences in our Applications". These applications include, but are not limited to, efforts to meet the policy requirements required by law or corporate policy. We would like you to share your learning curve with the Computer Security Community. We also encourage submission of papers on the following topics of high interest:

Systems Application

* Access Control Strategies

- * Achieving Network Security
- * Application of Trusted Technology
- * Integrating INFOSEC into Systems
- * User Experience with Trusted Systems
- * Secure Architectures
- * Securing Heterogeneous Networks
- * Small Systems Security

Criteria, Evaluation and Certification

- * Assurance and Analytic Techniques
- * Conducting Security Evaluations
- * Federal Computer Security Criteria
- * Experiences in Applying Verification
- * Integrity and Availability
- * Formal Policy Models

Management and Administration

- * Accrediting Information Systems and Networks
- * Specifying Computer Security Requirements
- * Life Cycle Management
- * Managing Risk
- * Role of Standards
- * Preparing Security Plans

International Computer Security Activities

- * Conformance Test Development and Evaluation
- * Harmonized Criteria
- * International Evaluation Infrastructure
- * Prototype Development
- * Research Activities

Innovations and New Products

- * Approved/Endorsed Products
- * Audit Reduction Tools and Techniques
- * Biometric Authentication
- * Data Base Security
- * Personal Identification and Authentication
- * Smart Card Applications
- * Tools and Technology

Awareness, Training and Education

- * Building Security Awareness
- * COMPUSEC Training: Curricula, Effectiveness, Media
- * Curriculum for Differing Levels of Users
- * Keeping Security In Step With Technology
- * Policies, Standards, and Guidelines
- * Understanding the Threat

Disaster Prevention and Recovery

- * Assurance of Service
- * Computer Viruses
- * Contingency Planning
- * Disaster Recovery
- * Malicious Code

* Survivability

Privacy and Ethical Issues

- * Computer Abuse/Misuse
- * Ethics in the Workplace
- * Laws
- * Privacy and Individual Rights
- * Relationship of Ethics to Technology
- * Standards of Ethics in Information Technology

We are pleased to invite academic Professors to recommend Student papers in the application of Computer Security methodology. Three student submissions will be selected by the Technical Committee for publication in the 14th NCS Conference Proceedings. To be considered, the submission must be solely authored by an individual student and be recommended by an Academic Professor. Only one copy for student submission is required.

BY FEBRUARY 15, 1991: Send eight copies of your draft paper* or panel suggestions to one of the following addresses. Include the topical category of your submission, author name(s), address, and telephone number on the cover sheet only. (* Government employees or those under Government sponsorship must so identify their papers.)

BY MAY 11, 1991: Speakers selected to participate in the conference will be notified when their camera-ready paper is due to the Conference Committee. All referee comments will be forwarded to the primary author at this time.

For additional information on submissions, please call (301) 850-0272.

Mailing Information:

1. FOR PAPERS SENT VIA U.S. or Foreign Government MAIL ONLY:

National Computer Security Conference ATTN: NCS Conference Secretary National Computer Security Center 9800 Savage Road Fort George G. Meade, MD 20755-6000

2. FOR PAPERS SENT VIA COMMERCIAL COURIER SERVICES (e.g.- UPS, FEDERAL EXPRESS, EMERY, etc.)

National Computer Security Conference c/o NCS Conference Secretary National Computer Security Center 911 Elkridge Landing Road Linthicum, MD 21090

Please note that the US Government Postal System does not deliver to Elkridge Landing Road.

3. FOR Electronic Mail: NCS_Conference@DOCKMASTER.NCSC.MIL (1 copy only; no figures or diagrams)

Preparation Instructions for the Authors

To assist the Technical Review Committee, the following is required for all submissions:

Page 1: Title of paper, submission, or panel suggestion

Focus & keywords (e.g. - Innovations and New Products - Biometric Authentication, Tools and Technology)

Author(s) Organization(s) Phone number(s) Net address(es), if available Point of Contact

Additionally, submissions sponsored by the U.S. Government must provide the following information:

U.S. Government Program Sponsor or Procuring Element

Contract number (if applicable)

U.S. Government Publication Release Authority

Note: Responsibility for U.S. Government pre-publication review lies with the author(s).

Page 2:

Title of paper or submission - do not include author(s) or organization(s) Abstract (with keywords)

The paper (Suggested Length: 8 pages, double columns, including figures and diagrams; pitch: no smaller than 8 point.)

A Technical Review Committee, composed of Government and Industry Computer Security experts, will referee submissions only for technical merit for publication and presentation at the National Computer Security (NCS) Conference. No classified submissions will be accepted for review.

The Conference Committee provides for a double "blind" refereeing. Please place your names and organizations on page 1 of your submission, as defined above. Failure to COMPLY with the instructions above may result in non-selection BEFORE the referee process.

Papers drafted as part of the author's official U.S. Government duties may not be subject to copyright. Papers submitted that are subject to copyright must be accompanied by a written assignment to the NCS Conference Committee or written authorization to publish and release the paper at the Committee's discretion. Papers selected for presentation at the NCS Conference requiring U.S. Government pre-publication review must include, with the submission of the final paper to the committee, a written release from the U.S. Government Department or Agency responsible for pre-publication review. Failure to comply may result in rescinding selection for publication and for presentation at the 14th NCS Conference.

Technical questions can be addressed to the NCS Conference Committee by mail (see Mailing Information) or by phone, (301) 850-0CSC [0272].


Search RISKS using swish-e

Report problems with the web pages to the maintainer



Jon Jacky <ON@GAFFER.RAD.WASHINGTON.EDU> Tue, 18 Dec 1990 10:09:53 PST

That's the headline for this story from THE SEATTLE TIMES, Dec. 17, 1990, p. A3:

COMPUTER MODELS LEAVE U.S. LEADERS SURE OF VICTORY by Robert C. Toth, Los Angeles Times

... Computer models of ground warfare convince the administration it can deliver on its promise of an overwhelming victory. An Army assessment of US and Soviet-made Iraqi equipment --- from tanks to rifles --- shows that the United States has an edge in quality to compensate for its numerical disadvantage. ...

When such assessments are factored into opposing ground-combat units and the forces are pitted against each other in war games, the conclusion by Pentagon

and many non-government experts seems to be the same: "We'd crush them," said Joshua Epstein of the Brookings Institution.

Iraqi numbers, including its million-man army, should not be a problem, added Barry Posen of the Massachusetts Institute of Technology. "If anything, we might begin to address the ethical question of how much slaughter you want to inflict on his forces if war comes." ...

Computer modelling for a ground war is based on assessments of the U.S. Army War Gaming Agency of the combat value and combat effectiveness of 10 types of weapons. ... Effectiveness ratings were determined for (... tanks and ...) other weapons categories from artillery to small arms. A rifle is valued at 1.0, a machine gun at 1.77, a 155 mm howitzer at 1.02 and a MLRS rocket system at 1.16. (... etc. ...)

The combat value, or relative weight, of the weapon categories were decided by a team of experienced battlefield commanders. Most valuable, they decided, are attack helicopters, followed by artillery, tanks, scaling down to small arms.

When the number of weapons in a U.S. armored division is multiplied by those effectiveness ratings and their combat value, the resulting total --- about 130,000 --- becomes the Armored Division Equivalent at 1. All other units can be measured against that standard. A U.S. infantry division, for example, is given an ADE of 0.5, or half an armored division.

Epstein and his associate, Alf Hutter, calculate that all U.S.-led forces in Saudi Arabia will be valued at 17.6 ADE's by February, when the buildup is completed. They calculate that Iraqi forces in Kuwait will be valued at 7.4 ADE's, and those in northern Kuwait and southern Iraq at 9.6 ADE's.

That appears to place opposing forces in balance, but the Iraqi forces are widely dispersed in defense, offering a challenge of only 2.3 ADE's for U.S. forces in the "main attack sector."

Epstein's bottom line, based on his modeling, is an 18-day war. The first six days would be used for air strikes to establish control and soften up Iraqi ground forces. In the next six days, the ground attack, breakthrough and movement northward would take place. The final six days would be used to mop up. Casualties would be about 15,000 (with 25 percent dead), he said, although they could range from 3,600 to 22,000.

Posen said such models understate the U.S. advantage because they do not reflect the better training, logistic supplies, command and control, and other qualitative edges. "We will have total control of the air," he said. ...

U.S. forces wil be able to concentrate at their intended attack point to reach a jump-off advantage of 5-1, Posen said, because of the U.S. expectation that Iraqi artillery --- the usual weapon to prevent such concentrations behind enemy lines --- will be largely wiped out.

"We are very good at counter-battery fire," he said, pointing to special radar to locate any Iraqi artillery batteries that could then be assaulted with massive, rapid-fire artillery weapons and the Multiple-Launch Rocket Systems. One MLRS volley of 12 rockets is supposed to have the same effect as 72 rounds of 155 mm howitzers.

"In just artillery alone, we figured we could delivery 500 tons of metal (artillery shells) on his positions in only one hour," Posen said. "We astonished ourselves with that figure."

- [And so on. There were a few caveats: "There are doubters... skeptics remain unpersuaded... experts warn that unpredictable events could turn the most modern technological projections into catastrophe ... JJ]
- Jon Jacky, University of Washington, Seattle jon@gaffer.rad.washington.edu

Re: Airline safety

Jim Rees <rees@citi.umich.edu> 11 Dec 1990 14:35 -0500 (Tuesday)

In <u>RISKS 10.67</u>, Donald A Norman writes a sermon on the Economist article concerning airline safety. He apparently didn't read the article itself and I wanted to clear up some things.

The suggestions in the Economist article were not advanced by the Economist. They were from Mr. Earl Weener, safety chief at Boeing. Weener did not urge the introduction of a new decision speed. He said that in two out of three accidents involving a go/abort decision on takeoff, the decision was wrong. [I find this hard to believe, since tossing a coin would give the correct answer more often. Maybe he just means the calculated V1 speed was wrong, not that the decision was wrong.]

Weener suggests improving the Ground Proximity Warning System (GPWS). The current GPWS is apparently not trustworthy, and accidents are caused when pilots ignore its warnings. Improving this system to the point where pilots feel they can trust it seems like a good idea to me.

Boeing's four suggestions -- better estimates of V1, better GPWS, ILS installed at more airports, and better use of flight data recorders -- all seem to me to be good ideas, although I also think that Mr. Norman is right in suggesting that a more comprehensive, systems approach is needed.

* The Incredible Lightness of Reference

Jerry Leichter <leichter@lrw.com> Tue, 11 Dec 90 09:27:53 EDT

My article on executives and PC's indicates the issue of Business Week that it was published in. Since Business Week is widely available, you can dig up the original article if you want more details or have doubts about the accuracy of my quotation.

Or can you? Like many mass-market periodicals today, Business Week takes

advantage of the flexibility of computer and printing technology to produce different editions for different audiences. The article I quoted appeared in the Bits and Bytes column of the Information Processing section. That section is part of the "Information Processing" pages specific to the "Industrial/Technology" edition that I receive. It may or may not appear in other editions; if it does appear, it may appear on different pages, under different headings, or even on different dates. Business Week has its own algorithms for deciding which edition to send you - they don't ask. (I suppose if you ask to be receive a particular one, they'll put you on the appropriate list.)

Anyone who has written an article citing information gleaned from a network posting knows that traditional citation techniques are not adequate for this new medium: Even a citation to a respected, broadly-read moderated list like RISKS would be very difficult for a traditional librarian to deal with, and most network postings are evanescent, archived nowhere and impossible to examine, much less verify, after the fact.

What's slipped in unnoticed is that the same technological mismatch has begun to apply for the seemingly traditional paper forms. Today, it's newspapers and magazines. Tomorrow, textbooks will be tailored to individual school districts, individual schools, even individual classes - a technology all the major textbook producers are working hard at introducing. Given that technology, perhaps we'll soon see different editions of novels, even of non-fiction works, tuned to regional differences in interest, dialect, social mores, or what have you.

The world network is supposed to be bringing us all together. In some ways, however, the same techology is acting to fragment our world: If everything is "narrow-cast" to more and more finely subdivided audiences, what do we share?

-- Jerry

✓ Unexpected effects of PC's

Jerry Leichter <leichter@lrw.com> Tue, 11 Dec 90 09:04:08 EDT

For Many Executives, PC's Mean More Typing -- and Less Managing

Some computer technology, such as automated teller machines, has made life easier. But in business, that's not necessarily so. A Georgia Institute of Technology study found that personal computers can make life harder for managers. The reason? When companies install PC's, they often cut back on support workers. So middle managers now spend a third of their time performing administrative tasks and only 25% managing, the study found.

"Companies think they're going to try to pay for technology by letting secretaries go," says Peter G. Sassone, the Georgia Tech economist who wrote the study. "But someone has to do the typing, filing, and copying." He says corporate buyers mistakenly think PC's can deliver the same degree of productivity improvement that mainframes brought to inventory and payroll jobs in the 1960's. And "computer companies still try to sell that same idea," he adds.

Ten to fifteen years ago, when word processing systems were starting to spread rapidly, I (and others) pointed out an interesting paradox: These systems were sold (and usually bought) as money savers. The idea was that you could get more work done with a smaller number of typists. In practice, the number of typists was unchanged; what actually changed was the quality (in some often hard to perceive sense) of the output: Since making changes was now so cheap, documents would go through many more revisions.

Well, it took a while but the original "purpose" of that equipment has reasserted itself - and this time it is being attained by management fiat.

Middle managers are particularly vulnerable since information processing technology has put so much pressure on them anyway. (I saw an estimate not long ago that there are some 25% fewer middle management jobs now than there were in 1985.) However, the trend is much broader. My wife is a lawyer who made the transition from a large Manhattan firm to an in-house counsel position for a very large industrial company about a year ago. One of the changes she had to adjust to was the lack of support staff: There is one secretary for three lawyers and several other professionals, and each person is expected to do most of the word processing for his own jobs. The comment from a friend - also a lawyer, but one very involved in the future of the profession - is that any lawyer starting out today had better learn to use a word processor; it'll be part of his job within a few years at most.

-- Jerry

✓ Long-distance printing, or the risks of being well-known

Jerry Leichter <leichter@lrw.com> Sat, 8 Dec 90 16:31:11 EDT

In a recent RISKS, Hank Nussbacher reports on printouts that were intended for a local printer in North Carolina but, due to a one-character error in specifying the receiving node, were regularly being printed in Israel. He's inspired me to write this note, which I've been meaning to get down one paper for quite some time.

There's an interesting class of risks in computer systems, particularly networked systems, that I call "the risks of being well known" - though I suppose "the risks of knowing too well" is better :-). The underlying problem is that the ability to easily address and reach a huge number of systems, without any built-in testing of the reasonableness of requests, can lead to some very interesting failures.

1. Digital sells a printer server known as the LPS40. This is a Postscript printer you stick on your Ethernet and then print to from a number of other machines on the net.

In order for your machines to be able to find the printer, you have to give it

a DECnet node name. In DECnet as it is today, the namespace involved is flat.

The LPS40 documentation had many examples in which the printer was addresses as node LPS40. If you don't think things through, and simply type the example startup commands as given, you will have a series of machines trying to send output to a printer named LPS40. This, indeed, happened at a number of sites at DEC several years ago.

If your local DECnet configuration has never heard of node LPS40, your attempts to start the software will fail. However, one of the first LPS40's at DEC, installed in Hudson, Mass., reserved that name; so it was in the standard configuration database distributed throughout the company. As a result, new sites all over the world found themselves printing files in Hudson.

As it happens, the protocol used for talking to an LPS40 is officially supported only over Ethernets, and won't work RELIABLY over wide-area nets but it will work SOMETIMES. When I heard this story, the record for long-distance printing was from somewhere in Georgia.

2. I'm not sure where I heard the following story; details would be welcome. The Andrew system, developed at CMU, provides a variety of network file services. At first, it was used only at CMU; later, CMU started distributing it to other universities. One university got the source code and started doing local modifications. Then they found their modifications mysteriously being removed - the system somehow migrated back to its old state.

Apparently, included with the source package was software to ensure that local copies of the system stayed up to date. On a regular (nightly?) basis, the software checked for local files that differed from those on a "reference" machine, and brought over "reference" copies if necessary.

Unfortunately, the "reference" machine was hard-coded as some machine at CMU!

3. Much simpler, but much more widespread: There have been many reports of FAX messages inadvertently sent to the wrong destination.

-- Jerry

✓ Organizational Aspects of Safety

Lance J. Hoffman <hoffman@eesun.gwu.edu> Tue, 18 Dec 90 14:07:27 EST

RISKS readers might be interested in "Organizational Aspects of Engineering Safety: The Case of Offshore Platforms" by M. Elisabeth Pate'-Cornell in SCIENCE Magazine, p. 1210 ff. of 30 November 1990. It describes how, while organizational errors are often at the root of failures of critical engineering systems, engineers tend to focus on technical solutions, in part because of the way risks and failures are analyzed. But, for example, in some systems described, improving design review costs two orders of magnitude less than adding steel to structures (the technical fix) to gain the same improvement in reliability. Prof. Lance J. Hoffman, Dept. of Electrical Engineering and Computer Science, The George Washington University, Washington, D. C. 20052 (202) 994-4955

[Also noted by haynes@ucscc.UCSC.EDU]

Covert communication through public databases

Larry Hunter <hunter@work.nlm.nih.gov> 18 Dec 90 17:39:19

This is not all that new, but I haven't seen discussion of the issue in RISKS, so I thought I would post excerpts from an interesting InfoWeek article (26 Nov 1990, pp.12-13):

[A] handful of major airlines - including American, United, Delta, and TWA - are being sued by almost three dozen plaintiffs who allege that the airlines use a shared database to "fix" prices and circumvent ... competition....

The ATPCO [Airline Tariff Publishing Co] database, critics allege, has become an electronic forum wherein airlines communicate with each other to keep ticket prices artificially high by discouraging competitive fares. A number of techniques are used by the carriers to signal one another, insiders say; for example, if a regional airline drops prices on a given route in an effort to boost traffic, a larger airline may slash fares on its flights in and out of the regional airline's hub airport, sending a strong signal that it disapproves of the smaller airline's new fares. The larger airline's low fares may remain in effect for only a day or two, but the other airline gets the message....

One airline spokesman acknowledged that airlines watch the database and closely respond to competitors' actions, but he calls that "the dynamics of the industry, not price fixing."

Ian Ayers, a faculty member at the law school at Northwestern University and a specialist in anti-trust cases, says: "The issue is, are the airlines just sharing data, or are they going beyond that and [through the database] talking about what they are going to do about the data?"

"Back in the good old days," says John Timmons, minority counsel to the Senate Commerce Committee and a close monitor of the airline industry, "if you were going to fix the price of something like steel, you'd make a phone call. Today, you'd use technology, but to my way of thinking, it's just like that phone call."...

Lawrence Hunter, PhD., National Library of Medicine, Bldg. 38A, MS-54 Bethesda. MD 20894 (301) 496-9300 hunter%nlm.nih.gov@nihcu (bitnet/earn)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mathematical Telephone Voting

<HMurray.Catwalk@DOCKMASTER.NCSC.MIL> Sat, 8 Dec 90 16:23 EST

>One risk that I don't think I saw mentioned in the discussion of >"Dial-A-Vote" systems relates to the identity of voters.

To the contrary, it has been dealt with ad nauseam, usually erroneously.

>Such a system, by definition, would need to know the identity of each caller >to check registration and avoid duplications.

This statement is patently false. While an identity-based system would be one way to accomplish these objectives, a voucher system would serve just as well. Such voucher systems are well described in the literature, but the same issue of RISKS which carried the above assertion, contained two descriptions of such systems for voting by mail. The problem of disassociating the vote from its origin, i.e. location of the phone, is much more resistant to solution.

All voting systems are subject to abuse, not the least are those systems currently in use. All voting systems have some problems of equity. In many of our current systems, these problems were deliberately engineered in for political motives. These problems resist solution precisely because any change will shift the political balance, however slightly.

To the extent that we can move to systems that are more secure, more equitable, and more economic, we should do so. Such systems clearly exist. My personal preference is for more equity. While I have difficulty in believing that any new system can be any more subject to abuse than most of those in use, I would be prepared to sacrifice some security for more equity, as long as the lower security would not result in a loss of confidence in the results.

Any new systems and the move to them will be fraught with problems. Much dialogue will have to precede any such moves. However, over-stating the problems of the new systems, preferring the faults of the old ones, and pandering to the fears of the ignorant are not productive.

William Hugh Murray, Executive Consultant, Information System Security 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

✓ Voting Technology

"William W. Plummer" <plummer@altacoma.wang.com> Mon, 17 Dec 1990 14:09:59 EST

I would like to propose a new voting system that will benefit from electronic and/or cryptographic techniques. Before going too public with this, I hope to get additional suggestions and pitfall information from you readers.

The voting system that I would like to see simply weights your vote by the number of tax dollars that you pay. We have often heard that the super wealthy use tax loopholes to lower their tax to zero while manipulating laws to make this possible. On the other end of the scale, the poor are accused of using tax supported services far in excess of their tax payments; the poor tend to vote for candidates that promise to keep up the handouts. Of course, it is the middle income people that support all of this. So, my scheme has the appropriate negative feedback built into it.

A major problem with the system is that it require a constitutional amendment. In other words we would no longer have "One man, one vote." But I argue that the Constitution was written before income tax and local taxes etc. In a sense everybody was taxed equally back then. All this new system does is to restore the equality of the voting power.

Implementing this system is tricky unless you want to trust "the government" to correctly credit your voting power. I think the ability to check one's own account is desired, but you really don't want it to become public knowledge;

worse than busybodies and neighbors would the the targeted marketing concerns and the politicians spending their resources where the voting power is. So, a secret ballot is still a must. The ballot must be unforgeable and not modifiable.

One idea that is almost right is to use public key crypto technology. The IRS would issue voting stickers which have the number of votes encrypted such that only the vote counters could read them. I would use my stickers by sticking them to a paper ballot; they could not be removed without destroying them. This fails because I cannot check that the sticker is worth the number of votes that I think it should be.

Making the stickers have duplicate information, one that the vote counters can read and one that I can read, is also almost right. It's a little impractical since it requires that I keep a decryption key around so that I can decode my half of the sticker. So, everybody has to be assigned a key and everybody has to avoid losing it.

Does anybody out there know how to do this? Thanks.

William W. Plummer Work: 508-967-4870 plummer@wang.com Home: 508-256-9570

Re: Hacked NASA phones (<u>RISKS-10.65</u>)

Barton Christopher Massey <bart@cs.uoregon.edu> Mon, 10 Dec 90 23:51:56 GMT

> [...] computer intruders have stolen some \$12 million in free telephone
 > service through Johnson Space Center... That figure was calculated from costs
 > of similar break-ins described by law enforcement agents specializing in
 > computer crime.

There *must* be some kind of mistake or error here, right? Imagine this principle applied to better-understood areas of criminal jurisprudence: "Little Johnny Nogood has stolen some \$2000 worth of goods from the corner store today... That figure was calculated from costs of similar thefts described by law enforcement agents specializing in shoplifting." Right. The whole thing is especially ludicrous in light of NASA's recent report that their whole yearly phone bill is only on the order of \$12 million...

The computer-related risk, IMHO, is that because the law-enforcement community doesn't understand computer crime, it may be made to seem much more harmful to its victims and to society than it actually is, and resources that would be better spent elsewhere will be devoted to stopping it. This risk is especially severe in light of the "computer crime experts" who have made a name for themselves because of the imputed significance of these kinds of cases, and thus have a vested interest in exaggerating their significance. Bart Massey

K Re: Response to article on "Legion of Doom" sentencing (<u>RISKS-10.65</u>)

Irving Wolfe <irv@happym.wa.com> 9 Dec 90 18:26:16 GMT

I, too, am opposed to uninvited access to others' computers.

In RISKS-10.65, we have

>Sorry. I don't buy it. If I leave my keys in my car with the windows open,>and you get in and drive off, you're still just as guilty of stealing the car

That is true. But it is also a crime in some states for you to have left the keys in the car. It is written in many insurance contracts, too, that the insurer will not have to pay you if you have encouraged the theft in this way.

Thus, in this other area of life that you drew an analogy to, your "asking for trouble" by making it easy and attractive does indeed reduce or eliminate your protection under the law or constitute a punishable minor crime itself.

> [several posters drew analogies to the crime of "breaking and entering"]

Breaking and entering is a crime that has two parts: "breaking" and "entering." If you leave your front door ajar, one need not "break" to "enter." If a company leaves the door to its office ajar, it cannot accuse an outsider found walking down its hallway (doing no harm) of any crime, it can only tell him to leave. Since people here seem so fond of analogies, I'll suggest that to the extent that a company leaves the door to its computer system ajar, the breaking and entering analogy fails, and the mere entry of an outsider would not constitute a crime.

These analogies are silly.

If we are to have a law in this area, it should be simple: Attempting to log into a computer system or otherwise access it without having been explicitly invited should be a crime whether or not the attempt succeeds and whether or not any damage was done. Probably using a normally-public area like an ftp or anonymous uucp directory should be explicitly excepted, as should a small number of attempts to log into a system accidentally, provided no hacker-type activities (systematically guessing passwords, taking advantage of system defects to gain privileged access, etc.) were involved.

But if this is to be a crime, it is fundamentally unrelated to old-time crimes like breaking and entering or car theft. We are making it a crime because we'd like to discourage it, not because there's a clear moral issue or any harm being done. There may or may not be. The law is for our convenience, and has no moral side, and the violator is not to be punished for his evil character, but merely for having violated a well-known law carrying a well-known penalty.

irv@happym.wa.com (Irving_Wolfe) Happy Man Corp. 206/463-9399 ext.101 4410 SW Point Robinson Road, Vashon Island, WA 98070-7399 fax ext.116 SOLID VALUE, the investment letter for Benj. Graham's intelligent investors Information free (sample \$20 check or credit card): email patty@happym.wa.com

Re: Legion of Doom (<u>RISKS-10.67</u>)

Mike Black <black@seismo.CSS.GOV> 9 Dec 90 13:18:40 GMT

In the discussions of the Legion of Doom a few points are raised but not taken to fruition seeing as how we are talking about a new technology (relatively new that is). Allow me to paraphrase:

1. "The company left its' doors open and that was a criminal act...". Response: "Leaving your garage door unlocked isn't".

Having a phone line into your company is definitely not a criminal act. However, if you leave a pile of money on the street and someone steals it, there isn't a judge in the world who would convict because you did something a reasonable person wouldn't have done. The problem crops up when you come with a new technology that has inherent risks. What the heck is a reasonable person...the two guys that invented it? On hacking, we have a case where technology allows extremely easy access to computers over phone lines. The fact that a company uses this technology does not relieve it of responsibility to behave as reasonable persons. The problem is that the hackers are perceived as a bunch of teenage hoods and they do not suffer from this technology. If every time one of them called they got electrocuted, I assure you that the company would be held liable.

2. "Leaving my keys in my car is not...". In most states, leaving the keys in your car is definitely considered criminal as you are inviting a crime. Doesn't then hooking an easy access phone line also invite a crime?

3. "We are in business to do business...". True, but businesses have a responsibility to society to ensure their business does not invite criminal behaviour.

4. "We shouldn't have to spend time closing known holes...". If I talked to your security department they might disagree. If there are known holes, is management adequately apprised of the potential for business loss and have they made a knowledgeable decision to not close them, or do the system managers just say, "The boss wouldn't understand so I'm not going to tell him"? Companies devote massive resources to security and this hacking thing is a new threat. So is the idea that your competitor could get in and muck about too. It would seem that a business shouldn't have to spend a lot of time closing security holes opened by a product they bought, so me thinks I would complain LOUDLY to whomever supplied this product to close up the holes.

5. Finally, let's try and define a reasonable person on this matter:

1. When you hook-up a phone line to your computer, a reasonable person would expect to get calls from unauthorized users.

2. A reasonable person would not expect the simple userid/passwd to foil everyone, however the same person should expect that a concerted effort not be made to overcome it. i.e. If you have userid "root"

with no password, that's unreasonable, most anything else migrates toward reasonableness.

3. A reasonable person would assume that one who finally got in would do most anything.

I propose the following:

1. All dial-up's contain a warning about the penalties of unauthorized entry. (virtually none do, how 'bout a trespass warning people?)

2. Entry into such a system would be a misdemeanor. Retrieval of info would be the same.

3. Damage caused would upgrade eventually to a felony depending on lost business, time to recover, etc. The trick here is the need to prove the hacker was proximate cause to the damage beyond reasonable doubt.

P.S. I personally do not support "hacking".

: usenet: black@beno.CSS.GOV : land line: 407-494-5853 : I want a computer: : real home: Melbourne, FL : home line: 407-242-8619 : that does it all!:

✓ Computer Virus as Military/Political Weapon?

Sanford Sherizen <0003965782@mcimail.com> Mon, 17 Dec 90 22:11 GMT

I would like to gather any *hard* evidence that viruses have been used for political/military purposes. It is possible that the Jerusalem virus was first set off to commemorate a Palestinian event but has there been any way to verify this? Are there other viruses that have been specifically distributed or directed to harm a political foe? It is important to differentiate this type of attack from someone setting off a virus that contains a political statement but which is not directed against a particular target. I know that this differentiation is soft but I am trying to develop an appropriate categorization. Any help on this is appreciated.

What got me thinking about this is my work on developing a model of computer crime trends and development stages. The current situation in the Persian Gulf made me wonder about the use of the virus as a political weapon. Is the virus a potential "small nation's weapon"? Can viruses become terrorist surrogates, disrupting an enemy nation without leaving direct fingerprints (strings?) traceable back to the ultimate sponsor? What roles could viruses play in future small scale intensive conflicts as well as major wars? Have viruses been considered in war scenarios that military commands have developed? The flap earlier this year about the availability of a small business contract to develop a virus for the U.S. military may well be part of a larger picture of computerized warfare joining other threats such as biological and chemical warfare.

Comments can be posted to me on Risks or sent directly to me at MCI MAIL: SSHERIZEN (396-5782). This message has also been posted to Virus-L.

Thanks, Sandy

Request for Information about Undergraduate Computer Security Classes

Al Arsenault <arsenaul@usafa.af.mil> Thu, 13 Dec 90 13:47:46 MST

We are requesting information from any and all colleges about Computer Security courses offered as part of the undergraduate Computer Science program. This information is needed as part of a research project on teaching Computer Security. The goal is to produce a summary of available courses, to be included in a paper we are writing.

The researchers involved are:

Alfred Arsenault, Visiting Professor of Computer Science, and

Captain Gregory White, Instructor of Computer Science,

both at the U. S. Air Force Academy.

Specifically, we are seeking answers to the following questions:

(1) Does your school offer a course in Computer Security as part of its undergraduate Computer Science curriculum? If so, what is the title of that course?

(2) If so, is the course required or an elective for Computer Science majors?

(3) What textbook is being used, if any?

(4) What are the prerequisites for the Computer Security course? (Please use descriptive titles, e.g., Operating Systems, rather than course numbers or designators.)

(5) Is the course offered once a year, or every semester?

(6) Approximately how many students typically enroll in the course?

(7) If your institution does not offer an undergraduate Computer Security course, is there a particular reason? (e.g., no faculty interest in teaching such a course; not enough students interested in taking such a course; no room in the undergraduate Computer Science curriculum for another course)

(8) Who is a point of contact that we can get in touch with if we need further information?

As previously stated, we are requesting this information to assist us with a research effort on "Teaching Computer Security in an Undergraduate Computer Science Curriculum." The short-term goal is to develop reasonably accurate statistics about how many institutions offer Computer Security courses. Negative responses (i.e., 'my college does not offer a Computer Security course') are welcome.

We would be happy to send summaries of the responses we receive to anyone who requests one.

Please send responses to either:

Alfred Arsenault: arsenaul@usafa.af.mil or AArsenault@Dockmaster.ncsc.mil

Greg White: white@usafa.af.mil GWhite@Dockmaster.ncsc.mil

If you have questions, or want more information, we can be reached on the net at the above addresses; by telephone at (719) 472-3590; or by U. S. Mail at

Department of Computer Science HQ USAFA/DFCS U. S. A. F. Academy, CO 80840



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Marcus J. Ranum <mjr@decuac.DEC.COM> Wed, 19 Dec 90 00:26:20 -0500

I've always been particularly interested in wargaming, and was really happy on the occasion I managed to game with a guy who also did occasional work with Navy wargames systems. His descriptions of how gaming parameters are derived may have been (I hope!) exaggerated, but I don't think I'd place much confidence in the results the games give. They may reflect a battle - but it's more likely the game will reflect the relative lobbying skills of the various groups who set the parameters. I gather that some arguments put forward run along the lines of:

"It's impossible to sink a carrier in this scenario," say the carrier drivers.

"Well, ok," reply the submariners, "then the probability of detecting a sub in case X is only Y%".

The end result is a game - but does it have anything to do with even the situation it is supposed to be simulating (which does not address the fact that in a real war, you are *never* presented with the situation you think you will be).

Apparently many of the parameters for weapons systems, etc, are drawn from manufacturer's specs, and the "actual" combat capability is extrapolated from published MTBFs, etc. This doesn't always take into account little things like grains of sand that may skew a value.

There's also the story of the wargame developed ("Firefight" by Jim Dunnigan I think it was) for the U.S. Army designed to train in infantry fire fight tactics. Apparently it was almost impossible by game rules for the OPFOR to win. (The game has been released as a commercial boardgame, with the values "fixed" - or "unfixed").

If you're interested in the subject, there's a pretty good book entitled, "_War_Games_", by Thomas B. Allen that glosses over the military's flirtation with game theory. It looks like another sad case of trying to make a "science" out of something, without having any real scientific way of quantifying the experimental subject. How *do* you make a meaningful statement about the result of a battle?

It sure would be rich if we learn years down the road that some white-tower theoretical soldiers in the Soviet Union were the REAL driving force behind perestroika because they couldn't get a 100% win in a conventional war simulation in Europe, because all their specs were drawn from the malarkey glossies defense contractors give the Pentagon.

mjr.

***** Re: Computer Models Leave U.S. Leaders Sure of Victory

Karl Lehenbauer <karl@ficc.ferranti.com> 19 Dec 90 09:34:58 CST (Wed)

No doubt this article is going to generate a lot of responses. Peter da Silva finds this reminiscent of the infamous Club Of Rome models that assigned pollution to a single numerical value and predicted that we'd all be dead by now.

Rolling the clock back twenty years or so, had the ADE been around we could be fairly certain that the assigned ADE of US Forces in Viet Nam far exceeded that of the enemy and that, therefore, a quick victory would be certain.

For a more recent example, consider that the ADE of the USSR forces

in Afghanistan surely exceeded that of the Afghan rebels, yet they lost.

-- uunet!sugar!ficc!karl (wk)

Kisks of believing war game models

"FIDLER::ESTELL" <estell%fidler.decnet@scfb.nwc.navy.mil> 19 Dec 90 10:04:00 PDT

A comment on the RISKS-FORUM Digest item of Tuesday 18 December 1990 RE: "Computer Models Leave U.S. Leaders Sure of Victory" is in order.

1. Computer models are usually naive, or even stupid. That does NOT necessarily mean that the one(s) cited in the referenced article were of poor quality; but it DOES mean that these models do NOT speak for intelligent, thoughtful PEOPLE - such as Gen. Colin Powell, Sec. Def. Dick Cheney, Senator San Nunn, etc.

2. How do I know that models are so often naive? First, I have read much available literature, from the RAND Corp., the GAO, etc. (e.g., "DOD SIMULATIONS: Improved Assessment Procedures Would Increase the Credibility of Results", GAO/PEMD-88-3, Dec. 1987; and "Analysis for Military Decisions", E.S. Quade, editor, Rand McNally & Co., 1964; and "Handbook of Systems Analysis", Hugh Miser and E.S. Quade, eds., North-Holland, 1988. Once you get into these, follow the trail that the bibliographies give. Like me, you can focus your interest, and still read three dozen books and conference papers.)

Moreover, I have used some of the "better regarded" models, including one that has been "certified" by the Navy. (I found and fixed several fatal bugs in the code; the model has not since been recertified.)

Finally, I have designed and written and used my own model; it is as "good" (based on comparison of results) as many of the better known larger, older models. I call it "Ape" because it mimics the others. It is robust and elegant, but no genius. In particular, it is subject to the "garbage in garbage out" syndrome; i.e., if you tell Ape that your aircraft cannot be shot down by their tanks, Ape will let you do that. Mother Nature may not; as the late Richard Feynman noted, She always enforces all of Her rules, even when we (scientists et al) forget.

3. In grad school, one my my profs had worked for Getty Oil, as an Ops Researcher. He told of the rivalry between the Getty half brothers. One had done a "study" to prove something; the other asked my prof to "... prove my brother wrong." They ran "their best model" and it said that the other brother was right; so, they "tuned" the input data and reran the model; and it still said the other brother was right; so ... on the 242nd retry, it finally said that the other brother was wrong. Remarkably, when these "results" (sans the history of 243 runs) were presented to J.P. Getty, he believed them, and cancelled the first brother's plans. Does DoD *ever* do things like that? You read the Wall Street Journal and Aviation Week articles about SDI, B-2, A-12, etc. and draw your own conclusions. My invitation to those so sure of success is, why not go over to Arabia and lead the troops to victory? You could be a hero?

Bob

✓ Compass Airlines disrupted by possible computer attack

Sarge <sarge@batserver.cs.uq.oz.au> 19 Dec 90 06:27:48 GMT

Compass Airlines, a new airline company in Australia (since deregulation a couple of weeks ago), has reported that there reservation system was being jammed. On one day alone 25,713 calls had been made.

The Chief Executive suspects a computer was used to repeatedly dial telephone numbers, which aborted when answered.

Note that they do NOT think any rival airline is involved.

Punny user interface

<[anonymous]> 19 Dec 90

While reviewing the design of an important control system, I came across the following (slightly edited):

"The OK flags are used to request operator input for an operation. If bit 2 is set by the operation, the keyboard control task displays a message, eg. OPERATION OK? If the operator types Y (yes), bit 1 is set. If (s)he types 9 (no - in German) bit 3 is set."

I don't know the full history of this decision to use "9" to represent "no", but it seems to me that someone with a fondness for puns and a lack of concern about the user interface managed to get a little joke included into the design. Please don't accuse me of lacking a sense of humour; if I had come across this in a game program I would have laughed heartily. But the user interface to a critical control system must be as clear and understandable as possible. An operator wanting to abort an operation should not have to remember that for this particular system, the opposite of "Y" is "9".

The field of computer programming abounds in little jokes like this. Some can actually be useful (eg. the little trash can on the Macintosh screen which bulges when full) but others are tiresome or actually dangerous. People who want to use computers to accomplish an important job should not have to learn all the "in" jokes of the fraternity of programmers.

Process control risks discussed in IEEE Software

Andy Oram <andyo@westford.ccur.com> Wed, 19 Dec 90 10:37:28 EST The following recent article should interest all RISKS readers:

Leveson, Nancy G., "The Challenge of Building Process-Control Software," IEEE Software, 7:6, November 1990, pp. 55-62.

Her subject matter touches on almost every application where a computer interacts with real-life activities -- including interaction with a user who supposedly has final control over the situation. Compared to some posters on this forum, her premise is an optimistic one: she takes for granted that computers should be used to control airplanes, factory production, power plants, etc. But she's very open about the difficulties of predicting and handling events.

The article includes some classic examples of computer-aided processes that went hay-wire. More significantly, she carefully tries to distinguish different levels of human and technological risk, and proposes research areas for dealing with each one.

I'm sure others have read this article, since it's in a major journal. Since I'm still a novice in the issues involved, I'd enjoy seeing comments -- please mail them to andyo@westford.ccur.com.

Andrew Oram, Concurrent Computer Corporation, One Technology Way, Westford, MA01886 (508) 392-2865{harvard,uunet,petsd}!masscomp!andyo

This is not an official statement from Concurrent, but my own opinion; therefore you can count on having one person who stands behind it.

✓ Unexpected effects of PC's

P.J. Karafiol <karafiol@husc8.harvard.edu> Wed, 19 Dec 90 11:55:29 -0400

In RISKS 10.59, Jerry Leichter says,

>each [lawyer] is expected to do most of the word processing for his own jobs.
>The comment from a friend - also a lawyer, but one very involved in the
>future of the profession - is that any lawyer starting out today had better
>learn to use a word processor; it'll be part of his job within a few years
>at most

I find this somewhat hard to believe. My father is a lawyer at a largish firm, and, indeed, many of the lawyers do some of their own word processing and are encouraged to know how to do it *in case of emergency*. But considering that the average lawyer there bills in the vicinity of \$150/hr (if not more!) and the secretaries bill \$30/hr to the client, most clients would rather the firm use more secretarial help than have lawyers spend precious time and money word processing. Since these billing schedules are even more skewed in the large NY firms, I hardly think that self-wordprocessing lawyers are going to be a major trend in the legal profession.

== pj karafiol

✓ Unexpected effects of PC's

<ark@research.att.com> Wed, 19 Dec 90 15:17:14 EST

I have a lawyer friend who told me that she is forbidden to use a computer, word processor, typewriter, or any other similar labor-saving device. The firm's rationale is that they charge by the hour.

Missing reference

Jerry Leichter <leichter@lrw.com> Wed, 19 Dec 90 09:09:12 EDT

An article of mine in <u>RISKS 10.69</u> referred to another article in the same issue, pointing out the difficulty of tracking down an apparently-solid bibliographic reference given in the latter. However, the second article didn't include the reference! Apparently it was lost in editing.

For completeness, that reference was: Business Week, 17 Dec 90, Page 96C/

-- Jerry

A semi-folk tale on the risks of being well-known

Daniel P Dern <ddern@world.std.com> Tue, 18 Dec 90 22:05:56 -0500

Jerry Leichter's (leichter@lrw.com) story on many printers within a network sharing the same name calls to mind a story I heard back when I was at BBN. This was in the period when the company was just starting to market/sell packet networks to commercial customers (i.e., private nets that weren't part of the ARPA/Internet). To initialize the IMP (older name for packet switch), the network installer made a tape from an active ARPAnet machine, and loaded that into the customer's single node.

I could all but hear this poor lonely packet switch waking up, as it were, and soliliquizing, "OK, I guess somebody had to restart me. Let's see who else is out there, and tell them I'm awake again. Hello? Hello? Is anyone out there? Hey, where is everybody? Dagnab, I'm a stub again... say, you don't suppose that war broke out and I'm the only one left do you? Ah, here's packets to handle! That's a relief. Yo! Guys! Anybody home! ..."

Sure, it worked. But how cruel...

Daniel Dern

Re: the risks of being well known (Leichter, RISKS-10.69)

Scott Schwartz <schwartz@groucho.cs.psu.edu> Tue, 18 Dec 90 23:37:53 EST

How many machines are there out there named, say, "vax1"? We have one here. There is one at the University of Delaware. I think Digital used to have one. Now of course these all have their names qualifed so that they are unique, but if you happen to have a friendly terminal server that caches recently accessed hosts, and also does name completion, then ``telnet vax1" may not get you where you expect to be.

On a related note, psuvax1 hasn't been a vax for many years, but the name has stayed the same: the machine gateways lots of mail and the system adminstrators wanted to avoid any surprises.

Ke: Organizational Aspects of Safety (Hoffman, <u>RISKS-10.69</u>)

Charlie Martin <crm@cs.duke.edu> Wed, 19 Dec 90 10:22:19 -0500

Lance Hoffman noted the SCIENCE article pointing out that the cost of fixing structural problems in drill rigs is two orders of magnitude greater than the cost of engineering reviews to catch the problems before construction. It's interesting that this is about the same cost saving reported in software engineering (errors caught early in design versus errors caught during O,E&M).

It looks like "it cost 1/100th as much to do it right as it costs to do it over" may be a general rule.

Does anyone know of similar cost data in other engineering fields?

Charlie Martin (...!mcnc!duke!crm, crm@summanulla.mc.duke.edu) O: NBSR/One University Place/Suite 250/Durham, NC 27707/919-490-1966

[By the way, I noticed yesterday that the ENTIRE Contents section was omitted from the distributed version of <u>RISKS-10.69</u>. I added it to the CRVAX archive copy. Sorry. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Richard Schroeppel <r@fermat.UUCP> Wed, 19 Dec 90 14:02:12 PST

My wife's reaction: Let's just hope Iraq is running the same simulation.

War Game Vendor, Telephone Support Service:
"Really? ... That's awful. ... I wonder how that happened. ...
What version are you running? ...
4.1.3? Oh, yeah, that version has a bug in the enemy tanks. Give me your address, and I'll send you the upgrade to 4.2. ...
Does who have it? ...
Probably; we sent out the upgrades three weeks ago. You should have gotten it by now. Did you send in your registration card? ..."

Rich Schroeppel rcs@la.tis.com

M The topic that wouldn't die: telephone voting

Brian Rice <rice@dg-rtp.dg.com> Mon, 17 Dec 90 16:33:50 est

>From the Associated Press (appeared in the News and Observer of Raleigh, N.C., 17 Dec 1990, p. 2B):

"WINSTON-SALEM, N.C.: State elections officials looking over November's balloting say voter fraud has tapered in recent years to 'tolerable' levels.

"State Elections Director Alex K. Brock says he foresees a day when North Carolinians will vote by telephone. Their voice patterns will be confirmed and their votes tallied by computer. [...]"

Aaack! These three sentences have got to be the most thoroughly alarming I've seen with my morning joe in years, even if I ignore the civil-liberties implications of "tolerable levels of voter fraud," or of making voting difficult without a phone, or even of the state's having (or thinking it has) every citizen's "voiceprint."

I 'spec I need to send Mr. Brock some back issues of the RISKS digest. It's alarming when a public official seems not at all to have thought about issues that seem obvious to you and me...and the most recent N.C. elections should have given him pause, his satisfaction with them notwithstanding.

Many RISKS readers will have been aware of a recent well-publicized race for office in North Carolina between candidates we'll call A and B. Now, candidate A has for quite some years referred to members of a certain ethnic group as the "bloc vote"--that is, against him--so it was not a surprise when reports surfaced after the election that members of A's party went to a precinct heavily populated by members of that ethnic group and methodically challenged every single voter's right to vote. This is an involved process, involving signatures of elections officials, sealed ballots, etc.; obviously this takes a while, and enormous delays were created, mitigating turnout.

I'm refraining from naming the candidates, parties, and ethnic groups involved because I'm not trying to make political hay (yes, I worked for B), because these reports have not been confirmed, and because the party-A folks were acting within the letter of the law. Nonetheless, Mr. Brock apparently hasn't heard the phrase "denial-of-service attack." Sigh.

Brian Rice, DG/UX Product Assurance Engineering Data General Corp., Research Triangle Park, N.C. rice@dg-rtp.dg.com +1 919 248-6328

Voting Technology

Jerry Leichter <leichter@lrw.com> Wed, 19 Dec 90 09:39:00 EDT William Plummer asks about cryptographic technology for implementing secure voting. (He also includes a long ramble about weighting voting by amount of taxes paid, a social and political issue that is completely independent of the technology used to implement elections.)

There are, in fact, algorithms to implement such votes. There are some very general algorithms allowing groups of mutually-distrustful people to reach a common decision. (One way such problems get posed in the theory community is as follows: The members of a millionaire's club are curious as to which of them is the wealthiest. However, they are also jealous of their privacy, so none is willing to reveal his actual wealth to any of the others. Devise an algorithm which will indicate which of them is the wealthiest, but which will reveal no other information about their wealth to anyone. Solutions to this problem exist. They are quite non-trivial!)

An algorithm designed specifically for voting was described in Josh Benaloh's PhD thesis. (Yale, 1987 or 88 I think.) In Benaloh's basic algorithm, we assume a central government and a public, broadcast network. People vote by posting various encrypted messages on the network. The protocol provides two guarantees: No voter can determine another voter's vote; the government cannot fake the outcome (i.e., any voter can look at the published data and, if the government cheated, determine that fact).

In the basic algorithm, the government can read anyone's vote. From this basic algorithm, Benaloh goes on to show how to get by without a trusted government - essentially, one can split the government's responsibilities up among a number of independent agents in such a way that only the collusion of ALL the agents would allow a vote to be read. (The idea is that you would choose to do your voting through the Democratic, Republican, and Libertarian Party clearing-houses, plus for good measure the ACLU and the NRA, figuring that if ALL of them are allied against you, there's not much point in worrying about trivialities like vote privacy.)

Finally, Benaloh shows how to construct an election which reveals only the minimum of information: Who won, but nothing at all about the vote totals.

Again, the techniques involved are mathematically quite sophisticated. (They are closely related to RSA, but not identical to it.) They are all "efficient" in the theoretician's sense (polynomial time), but not (yet?) practical for a real, large election.

If you want further information, at last word mail to benaloh@cs.yale.edu was still being forwarded.

-- Jerry

Re: Voting Technology

"Michael J. Chinni, SMCAR-CCS-E" <mchinni@PICA.ARMY.MIL> Wed, 19 Dec 90 13:05:05 EST

>From "William W. Plummer" <plummer@altacoma.wang.com>:> The voting system that I would like to see simply weights your vote

> by the number of tax dollars that you pay. We have often heard that the

> super wealthy use tax loopholes to lower their tax to zero while manipulating

> laws to make this possible. On the other end of the scale, the poor are

> accused of using tax supported services far in excess of their tax payments;

> the poor tend to vote for candidates that promise to keep up the handouts.

> Of course, it is the middle income people that support all of this. So, my

> scheme has the appropriate negative feedback built into it.

Yeah, negative feedback. TO MUCH NEGATIVE FEEDBACK.

The MAJOR problem with your scheme is that government under it would only represent those with the most money (the rich). If your plan was made law, I foresee the rich changing their tax-status and doing their tax-returns so that they are taxed the most. This gives them enough votes to elect ANYONE they want. Regardless of the votes of everyone else. This then makes our country no longer a democracy ruled by the will of the majority, but a country ruled by a priviledged few (kind of what england was like before the Magna Carta or what South Africa is like now). What possible results would this have for the non-priviledged few. Results like:

result why

no labor laws costly (gives the employee more money and hence more voting power)

no financial aid for college costly (more smarts and people might realize that they have effectively no

say in the way they are governed)

The idea being that everything that has made the life (working and private) of the middle and lower classes better, that is funded by the government or was made possible only by government regulation, would be done away with if it interfered with what the rich wanted.

End result - the rich get richer and more powerful and

the middle and lower classes become one class - the lower class

> A major problem with the system is that it require a constitutional
 > amendment. In other words we would no longer have "One man, one vote." But I
 > argue that the Constitution was written before income tax and local taxes
 > etc. In a sense everybody was taxed equally back then. All this new system
 > does is to restore the equality of the voting power.

Back then it wasn't so much as tax equality as it was to insure that those being governed had an effective way to decide how they would be governed.

(insert standard disclaimer here)!uunet!pica.army.mil!mchinni Michael J. Chinni, Simulation Techniques and Workplace Automation Team, US Army Armament Research, Development, and Engineering Center, Picatinny Arsenal, NJ

🗡 telephone voting

Lauren Weinstein <lauren@vortex.com> Tue, 18 Dec 90 18:50:53 PST

In a recent digest, a contributor quoted (without attribution) from an original Risks message of mine which pointed out some potential problems with "Dial-A-Vote" systems--particularly in regards to identity issues. He used

phrases such as "patently false" and "pandering to the fears of the ignorant", and seemed to feel that other messages pointing out ways to do physical mail voucher voting invalidated the concerns.

I'd like to point out that my original message was clearly oriented *specifically* toward the issues of telephone-based voting systems. I was not discussing physical mail-based systems. The author admitted that the issue of disassociating the vote from its origin in a telephone-based system was a serious problem. That's the whole point of my original message! Given the realities of modern telephone technology, there is no way for users of such a system to be sure that their telephone number, and thus their address, has not been tagged by the voting system. Even if the system doesn't need to differentiate among voters in a multi-voter household, the simple capability of automatically correlating vote with voter location should trigger the Risks alarm bells. Anyone who thinks that significant numbers of voters will bother to vote from payphones (assuming such is possible) to avoid such problems is dreaming!

Finally, I don't consider pointing out these concerns to be "pandering to the ignorant". Even when there is a theoretical way to do the job right (which isn't always the case), the way the job may actually be done may not avail itself of the correct techniques, in the interests of time, money, or other factors. Unfortunately, it's all too easy for such systems to be made to "sell to the gullible", particularly when attempts are made, however benignly, to minimize discussion of the potential problems involved.

--Lauren--

Re: Response by Legion of Doom

John Boyd;CRENP <johnboyd@logdis1.oc.aflc.af.mil> Wed Dec 19 10:29:41 1990

>Date: 9 Dec 90 18:26:16 GMT

>From: irv@happym.wa.com (Irving Wolfe)
>Breaking and entering is a crime that has two parts: "breaking" and
"entering." If you leave your front door ajar, one need not "break" to
"enter." If a company leaves the door to its office ajar, it cannot accuse an
>outsider found walking down its hallway (doing no harm) of any crime, it can
>only tell him to leave.

Isn't this trespassing? If I arrive home with an armload of groceries, unlock the front door, take say, three steps and set the groceries on the floor, and turn to lock my door and find you standing in my living room, you'll stand a good chance of either getting your butt kicked or shot!

From: black@seismo.CSS.GOV (Mike Black)

>3. "We are in business to do business...". True, but businesses have a
 >responsibility to society to ensure their business does not invite criminal
 >behaviour.

And don't people in general have a responsibility to society to behave in

acceptable, legal ways? 'The devil made me do it' was never a defense. So far, I don't think the phone companies have been sued as being a party to bookmaking operations.

>5. Finally, let's try and define a reasonable person on this matter:

>1. When you hook-up a phone line to your computer, a reasonable>person would expect to get calls from unauthorized users.

And a reasonable person would expect the company that wrote the software to have made _reasonable_ efforts to defeat entries by those unauthorized users (hard-core, criminal hackers notwithstanding). But then, they've already taken themselves off the hook with those legalese non-warranties.

johnboyd@ocdis01.af.mil

Disclaimer - If I express an opinion, the Air Force will deny I know what I'm talking about.

Ke: Response to "Legion of Doom" (Wolfe, <u>RISKS-10.70</u>)

K. M. Sandberg <sandberg@ipla01.hac.com> 19 Dec 90 16:37:46 GMT

>Breaking and entering is a crime that has two parts: "breaking" and >"entering." If you leave your front door ajar, one need not "break" to >"enter." If a company leaves the door to its office ajar, it cannot accuse an >outsider found walking down its hallway (doing no harm) of any crime, it can >only tell him to leave. Since people here seem so fond of analogies, I'll >These analogies are silly.

How about trespassing? Actually breaking and entering is a good analogy because most computer systems do have a lock, the passwords and accounts, but they are not very strong, like houses. To have not password would be like leaving the door unlocked, but how many companies do this? Cars are also the same, dare you say that leaving a nice car around where someone can see it it causing an it to be stolen? The solution: get rid of everything that might attract someone. Is this what you want?

Just how strong of a lock must you have before you are no longer accused of making it easy for someone to break in?

>If we are to have a law in this area, it should be simple: Attempting to log
into a computer system or otherwise access it without having been explicitly
invited should be a crime whether or not the attempt succeeds and whether or
>not any damage was done. Probably using a normally-public area like an ftp
>or anonymous uucp directory should be explicitly excepted, as should a small
>number of attempts to log into a system accidentally, provided no hacker-type
>activities (systematically guessing passwords, taking advantage of system
>defects to gain privileged access, etc.) were involved.

>

>But if this is to be a crime, it is fundamentally unrelated to old-time crimes >like breaking and entering or car theft. We are making it a crime because >we'd like to discourage it, not because there's a clear moral issue or any >harm being done. There may or may not be. The law is for our convenience, >and has no moral side, and the violator is not to be punished for his evil >character, but merely for having violated a well-known law carrying a >well-known penalty.

I'm sorry, but I do think that breaking in to a computer has a moral side. People should take responsibility for their own actions and know that something is wrong and not just because of a law. Society can not, nor should not in my opinion, make a law for every possible thing that can or will be done. A person has to be reasonable and for someone to say that they did not think that breaking into a computer system (getting around the password protection at least) was not wrong is being unreasonable, besides if they didn't think it was wrong, why do they hide the fact that they are doing it?

On the computer systems I have been responsible for I have put a notice on login "Unauthorize access is prohibited", which makes it clear that unless you are authorized, you don't belong on the system. Even use by employees can be questioned if they use the system for non-work related things that impact the system, but this is not the intent.

Kemasa.

It would be interesting if people would listen to what they are saying, but then again others are not listening either, so why should they?

Ke: Response to article on "Legion of Doom" sentencing

Brendan Kehoe <brendan@cs.widener.edu> Wed, 19 Dec 90 14:34:29 GMT

In <u>Risks digest 10.70</u>, Irving Wolfe (irv@happym.wa.com) wrote:

> Attempting to log into a computer system or otherwise access it
 > without having been explicitly invited should be a crime whether or
 > not the attempt succeeds and whether or not any damage was done.

How in the world would such a thing be enforced? Agreed, you'd have to give leeway for the cases like ftp/uucp, accidental attempts, etc. But trying to word such a law would be sheer hell -- the number of loopholes that'd be created would far outweigh the number of benefits. For example: just last night, someone tried to log in as root through FTP to one of my machines. How would this fall under these guidelines? It's an FTP session, so it's got the shadow of "exempt" hanging above it. But wait! It was an attempted login to *the* privileged account, right? True. But the person could easily say they were root on their own machine (assuming it was the same person) and they just hit &eturn> at the name: prompt before they realized what they were doing, and subsequently were stuck with logging the FAILED LOGIN message. A really messy situation.

I completely agree that there should be some sort of law concerning this issue, even moreso in recent months (with the # of attempted logins from unrestricted terminal servers on the rise). But trying to make such a law real would be dangerously close to constantly monitoring every connection for anything that some "objective party" deems suspicious.

>But if this is to be a crime, it is fundamentally unrelated to old-time crimes >like breaking and entering or car theft. We are making it a crime because >we'd like to discourage it, not because there's a clear moral issue or any >harm being done. There may or may not be.

Exactly. We're trying to take a law that restricts walking pets in the park and make it apply to bringing your adorable scorpion "Spike" for a little jaunt down the block.

Brendan Kehoe - Widener Sun Network Manager - brendan@cs.widener.edu

Value of data integrity

&ahan_Stephen@lanmail.ncsc.navy.mil> Wed, 19 Dec 90 10:16:00 CST

I have a few thoughts on the ideas expressed [in <u>RISKS-10.66</u>?] about "no damage being done by an unauthorized user".

The data in a computer has value. This applies to software under development, experimental records, financial records, and almost all other forms of electronically recorded data.

A large part of the value of the data lies in the knowledge of the integrity of the data and the confidence placed in the data as a result. If an unauthorized used has gained the ability to change the information in the computer then REGARDLESS of whether any information was actually changed the degree of confidence in this information is necessarily lessened.

Restoring the original level of confidence in the data will require some finite amount of effort, whether restoring from backups, reconstructing, comparing against old printouts, or other techniques. The amount of effort depends on the value of the data and the willingness to accept a lesser confidence level, as well as other implementation dependent details.

Viewed in this respect, unauthorized access to the system does result in losses to the owners of the system whether or not any alteration of the information took place.

These are my opinions only and do not necessarily represent any other person or organization.

Stephen Mahan, Naval Coastal Systems Center, Panama City, FL 32407-5000





MERO - Hazard of Electromagnetic Radiation to Ordnance

Rodney Hoffman &offman.El_Segundo@Xerox.com> Fri, 21 Dec 1990 13:47:30 PST

Summary of a 30-column-inch article in the Dec. 21, 1990 'Los Angeles Reader' (see final paragraphs below):

WORLD'S MOST ADVANCED ARMY IS IN DANGER OF ZAPPING ITSELF

The Hazard of Electromagnetic Radiation to Ordnance, Or, How an Electronic Accident Could Ignite a Gulf War

By Patricia Axelrod and Capt. Daniel Curtis (USAF Ret.)

HERO, a feature of the electronic battlefield the Pentagon prefers to keep secret, can launch a rocket or crash a plane without warning. During the Libyan air strike, it caused an American fighter bomber to crash and

accidentally bomb friendly embassies and residences.

USAF Col. Charles Quisenberry says electronic emissions from US weapons "were interfering with each other" in the Libyan attack, and that "we did it [the mishaps] to ourselves." He also blames HERO for a series of UH-60 Black Hawk Army helicopter crashes.

Quisenberry is conducting a classified 3-year study of HERO called the Joint Electromagnetic Interference Study -- JEMI. Quisenberry says preliminary JEMI findings are that combinations of US weapons transmitting radio waves at certain frequencies can bring down an aircraft by putting it into an uncommanded turn or dive or by turning off its fuel supply.

The Pentagon classifies the electroexplosive device (EED), as especially HERO-prone. The EED is used universally throughout the weapons industry as a fuse trigger, activating everything from artillery to nuclear missiles. Charles Cormack, Navy EED specialist, claims that the EED has caused 25 weapons accidents, but civilian experts believe that there have been many more. Defective wiring such as "Kapton," which can cause HERO, is reported to be used on more than 50 types of aerospace vehicles.

Among many possible HERO-caused accidental firings, explosions, bombings, crashes, etc., a worst case scenario might be the accidental explosion of a Tomahawk or other nuclear device. The electromagnetic pulse following such an explosion could then trigger HERO chain reactions.

---- [end of article summary]

The 'Los Angeles Reader' is a weekly give-away not generally known for its hard news coverage, nor for any attempt at "balance" in its stories.

At the end of the article I've excerpted, an editorial note says it "is based on ... findings extracted from personal interviews ... government and military documents, accident and mishap reports released through the Freedom of Information Act, and newspaper and journal articles, and expert research papers. It was made possible in part by a grant from The John D. and Catherine T. MacArthur Foundation ... for Research in Peace, Security and International Co-operation."

[Los Angeles Readers not to be confused with Los Angeles Raiders, who have a newly regained electromagnetic pulse each week. PGN]

WA E-mail Privacy Suit

Peter Marshall <peterm@halcyon.UUCP> Wed, 19 Dec 90 09:32:40 PST

>From Jim Simon, "Computer Privacy at Issue in Suit," THE SEATTLE TIMES, 9/17/90, D1:

Like thousands of other state employees, Ron Collins figured the confidential computer messages he sent...couldn't be read by his bosses or anyone else.

He figured wrong.

The agency[Labor & Industries]in what officials say was an unprecedented monitoring of a state employee's private computer files, secretly retrieved and copied Collins' "electronic mail" messages as part of an investigation into whether he was improperly using state computers. In turn, Collins and the Washington Federation of State Employees filed suit last week...alleging the agency violated state privacy statutes, including those preventing wiretapping or other electronic surveillance without a court order.... the Collins case is already attracting national attention....

"We're in an era where every advance in technology means that each case like this brings us to the next frontier of privacy laws," says Sharon Beckman, an attorney for the...Electronic Frontier Foundation.... Collins...came under scrutiny in June after a supervisor noticed a message written by him on an open computer screen. Joe Dear, director of labor and industries, said the message prompted such concern that the agency--after getting approval from the state attorney general's office--had the Department of Information Services retrieve all of Collins' messages in early June....

Union officials said workers were never told the system couldn't be used for personal messages. They note that the use of electronic mail--a system known as PROFS and used by 3,000 state employees--requires a password.... "I think this is going way overboard, way too intrusive," said Gary Moore, head of the state employees union....

Collins' suit is one of a handful of of similar cases around the nation.... The problem, many observers say, is that privacy laws designed for telephones and telegraphs are being made obsolete by telecommunications advances. Privacy advocates around the nation have battled against caller-identification telephone programs, and observers say voice-mail systems could wind up as susceptible to employer snooping as E-mail.... The American Civil Liberties Union has sought federal laws preventing employers from monitoring employees' private computer files. And Dear concedes the Collins case should prompt agencies to write more explicit rules....

[Update: ...and, indeed, just that appears to be in the works now in Olympia, the state capital. With the lead taken by the Dept. of Information Services, who had no relevant rules in place before the Collins case, the Gov.'s Cabinet is developing rules expected to take final form in an Executive Order. The Collins case, however, is still in process.]

Process control risks discussed in IEEE Software (Oram, <u>RISKS-10.72</u>)

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Wed, 19 Dec 90 15:47:19 -0800

Compared to some posters on this forum, [Leveson's] premise is an optimistic one: she takes for granted that computers should be used to control airplanes, factory production, power plants, etc. But she's very open about the difficulties of predicting and handling events.

I guess I wasn't very clear in my Nov 90 IEEE Software article. Actually, I am more of a cynic than an optimist -- I take for granted that computers will (vs. should) be used in process-control and try to present some research topics that need to be addressed (it was an invited paper on challenges for the 90's).
An article that deals more directly with software safety and techniques to try to reduce risk will appear in the February issue of CACM (it was supposed to appear side-by-side with and as an alternative viewpoint to Dave Parnas' article last May but somehow got delayed in press).

nancy leveson

Ke: "Computer Models Leave U.S. Leaders Sure of Victory"

Peter G. Capek <APEK@YKTVMT.BITNET> Wed, 19 Dec 90 23:07:24 EST

A colleague used to have a sign on his office wall which said roughly:

"A model is an artifice for helping you convince yourself that you understand more about a system than you do."

Enough said.

Peter Capek -- IBM Research

"Computer Models Leave U.S. Leaders Sure of Victory" (<u>RISKS-10.69</u>)

The Polymath <hollombe@ttidca.tti.com> 20 Dec 90 01:57:12 GMT

A friend of mine (name omitted for his protection) is a contract programmer who worked on one of these models for over 5 years. It's his opinion that parts of the model had been deliberately tweaked to "tell the generals what they want to hear." i.e.: That their equipment works as advertised, so they'll win. Model results can then be used to justify purchase of more of the same equipment.

If things continue as they are, we may well find out if it matters in the real world.

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

Ke: "Computer Models Leave U.S. Leaders Sure of Victory"

Neil Galarneau <neil@progress.com> Thu, 20 Dec 90 14:44:30 GMT

An excellent book on the topic that has come out recently is Peter Perla's _____The Art of Wargaming_

The book deals with both the military and commercial sides of the topic. He mentions some problems the Japanese had in wargaming the Battle of Midway, for example.

Neil

P.S. For those who are curious, the referee of the wargame (a Japanese admiral) pointed out to the Japanese team that although they had won, they had no plans for dealing with the American fleet if it was north-west(?) of Midway.

Due to cryptanalysis, guess where we were? :-)

Kisks of Automated Collections and a Happy Ending

Lance J. Hoffman <hoffman@eesun.gwu.edu> Thu, 20 Dec 90 13:52:29 EST

Recently, I had a run-in with my bank which had a happy ending. The letters between me and it are self-explanatory, so, without further ado:

LETTER FROM ME TO BANK ON NOVEMBER 28, 1990:

Mr. (name deleted) President (bank name and address)

Dear Mr. (name deleted):

I am a professor of computer science at The George Washington University. I want to thank you for giving me an example of an insensitive and counterproductive computer-aided system to discuss with my classes. Let me explain.

Yesterday evening, I received a telephone call at approximately 6:50 p.m. from your credit collection department. A human operator asked for me and then, when I identified myself, played a taped message asking me to pay my Visa bill (account number (deleted), after which the connection was broken.

The tape stated that my account was overdue, despite the fact that when I called two days ago, I was told it was current. I had been away for a month or so and when I returned last week I immediately mailed in the complete payment for the old overdue bill and then, a day later, I mailed in a complete payment for the newly arrived and current bill. Since I received an overdue notice in the mail early this week and a(nother) phone call from a human on my recording machine, I called back. By that time, you must have received one of my payments at least, since I was told (three days ago) that my account was current!

At about 9:50 a.m. this morning, I talked with Ms. (name deleted) of your customer service department. She was pleasant, understanding, volunteered that I had a valid point, and knew how the system operated. (That's where I got the bank president's name -- LH) According to her, if a bill is not paid by me by the 17th of a month, I will get a recorded call from the Collections system, even if my payment is received in the intervening time. (Your bank) obviously

doesn't care enough to fax to the human operator who initiates the call a list of "late pays, now current", and would rather have people like me tell my friends horror stories about (your bank).

I don't enjoy having my dinner interrupted by taped messages, especially when your right hand apparently doesn't know what your left hand is doing. Whatever bozo put in this telephoning system should be demoted, after being called at dinnertime every day for a month. He or she would have been lucky to pass with a low D any system design course I taught!

I have now stopped telling my friends about the 1% rebate (a definite plus for your Visa card); they can give their business to whatever bank they want, as far as I am concerned.

I think your action is especially uncalled for since my record in the past is exemplary in paying my bills, including yours. I think you owe me an apology. Moreover, I think your recording may violate harassment provisions of the Fair Credit Reporting Act or some other federal law; by copy of this letter, I am asking my attorney for a quick opinion.

To date this year, I have written \$(amount deleted) in checks to your bank in payment of my Visa bills:

(I inserted a transaction log here, generated by Quicken)

I think such a customer deserves more consideration than your "system" gives him, and I hope you take steps to change it.

Sincerely,

Lance J. Hoffman

c: (name deleted), Manager, Collections (name deleted), Supervisor, Customer Service (name of a friend who is an attorney), Esq.

* * * * BANK'S RESPONSE DATED DECEMBER 13, 1990, RECEIVED DECEMBER 20, 1990

Dear Mr. Hoffman:

Your letter to (bank president) has been referred to me as I am directly responsible for the Collections Department. ...

[The Collection Recording System's] scheduling of the recorded call is designed to allow sufficient time for our customers to submit a payment before their account reaches 30 days past due. ...

The taped messages were scheduled to be made on November 19th, 20th, and 21st. Regrettably, our processor (which type?!-LJH) did not begin calling until November 27th. ...

Your letter has prompted us to reanalyze the entire program. As stated earlier its purpose is to serve as a friendly reminder for payment. Its (sic) obvious, however, that any delays that may occur in the future will only serve to offend our good customers such as yourself. Therefore, we've decided to phase out the Collection Recording System within the next three months.

I sincerely apologize ...

(name deleted) Group Vice President (bank) Card Center

It's nice to see that sometimes one well-aimed missive can change things.

Professor Lance J. Hoffman, Department of Electrical Engineering and Computer Science, The George Washington University, Washington, D. C. 20052 202-994-4955

Re: The topic that wouldn't die: telephone voting

Gregory G. Woodbury <ggw%wolves@cs.duke.edu> Thu, 20 Dec 90 19:28:05 GMT

Brian Rice notes that the Directory of the NC State Board of Elections forsees a day when big brother will have everyone marked by voiceprint.

Fortunately, not all of the folks here are going to take his comments seriously. The NC legislature has to make any changes to the system and they are NOT inclined to trust technology.

A few years back, the NC House of Representatives installed an electronic voting system in response to public pressure to provide more accountability. It has taken them nearly 10 years to get used to it.

As for the challenging of all votes by a certain candidates workers in some precincts: the process of challenging a voter in NC is specific and costly. An incorrect challenge costs the challenger cash and personal court appearances when the challenge is overturned.

Following the severe problems with the machines in Durham and Guilford counties, there have been all sorts of stories trying to account for why these two counties had all the problems. The latest reports that I have heard from the Durham BoE confirmed my earlier report that these two counties had some specific changes in the way the voting machines were to be programmed that were not anticipated as leaving the machines vulnerable to jamming.

In both counties, there was ONE independent candidate for a partisan office that had a relatively full slate in each of the two main parties. In this case it seems that the way the machines are physically linked in the back had only one long and inadequate lever connecting the third row to the interlock section. Voting for a full complement in the main parties and then also selecting the independent candidate would spring the interlock section for that race and render the machine unuseable until the mechanics could get there and unjam the machine.

In my precinct, we spotted the inoperative machines very quickly and quit using them until they could be fixed. In other precincts it was reported that the malfunctions were not noticed until several voters had used the malfunctioning machines.

There are rumours that this jamming may have been deliberatly caused by some (unknown) party's instructing voters how to jam the machines, but there is no confirmation of this that I am aware of.

Gregory G. Woodbury @ The Wolves Den UNIX, Durham NC ggw%wolves@mcnc.mcnc.org UUCP: ...dukcds!wolves!ggw ...mcnc!wolves!ggw



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Curtis Jackson <jackson@adobe.UUCP> 2 Jan 91 22:48:02 GMT

While vacationing in Honolulu last week, my fiance and I had the misfortune to run into a very vicious failure recovery mode in an elevator in our hotel. As near as I could tell, the elevator doors did not have the usual leading-edge vertical strip which, when depressed horizontally, causes the doors to open so as not to crush a person or appendage. Instead, this function was relegated entirely to an "electronic eye" beam.

One particular elevator was malfunctioning -- closing only partially before jerking open as if someone had broken the beam. But regardless, if the doors on any elevator attempted to close for four times without success due to the beam being broken (or due to a faulty perception that the beam was being broken), it would buzz loudly as it closed the doors slowly and completely. During this final closure, presumably to prevent someone from standing in the doorway and monopolizing the elevator on one floor, the doors would close regardless of what the electronic eye told them. I tested this by placing my shoulder between the doors (an action that normally always opened the doors because I broke the beam), and the doors continued to close onto my shoulder and then made a meaningful attempt to crush my shoulder. The DOOR OPEN button had no effect when the elevator was in this close-at-all-costs recovery mode.

My first thought was what would happen to someone who slipped on the doorsill of the elevator and injured themselves. The doors would attempt to close several times, then buzz at the poor sod as they attempted to crush him/her in the doors. Even if the elevator had not been programmed to ignore the beam in this mode, I would still find the lack of a physical means to override the door closure (the traditional leading-edge strip) to be a severe safety hazard.

Curtis Jackson @ Adobe Systems in Mountain View, CA (415-962-4905) uucp: ...!{apple|decwrl|sun}!adobe!jackson

Dehumanization by old Cobol programs; how to get 4x as much junk mail

Darrell Long <darrell@sequoia.ucsc.edu> Wed, 26 Dec 90 10:29:14 PST

My dear mother blessed (or perhaps cursed) all of her children with two middle initials, in my case "D" and "E". This has caused me a good deal of trouble, as you can imagine.

It seems that TRW (and now we learn Lotus) sells certain parts of you credit information, such as your name and a demographic profile. Well, I recently got a new credit card from Gottchalks and found to my chagrin that my name had been truncated to "Darrell D. Long". I went to the credit manager and patiently explained my situation, and was assured that things would be fixed and they were very sorry etc, etc.

Well, two things happened: I got a new credit card, this time as "Darrell E. Long", and TRW now has an annotation in my file to the effect "File variation: middle initial is `E'". Soon after this I start getting mail for "Darrell E. Long" (along with the usual "Darrell Long" and "Darrell D. Long" and the occasional "Darrell D. E. Long").

I called up the credit bureau and it seems that the programmer who coded up the TRW database decided that all good Americans are entitled to only one middle initial. As the woman on the phone patiently told me "They only allocated enough megabytes [sic] in the system for one middle initial, and it would

probably be awfully hard to change."

I know I'm not the only one with more than one middle initial -- of my european friends have several. I wonder what they do with a name like "Ananthanarayanan", do they randomly truncate it? -- I suppose I should my friend.

I'm afraid it's going to get worse before it gets better though. With Lotus' product such name mutilation will only spread. DL

Dr. Darrell D. E. Long, University of California at Santa Cruz

"Computer data putting history out of reach"

"Jay Elinsky" <LINSKY@YKTVMZ.BITNET> Wed, 2 Jan 91 14:11:38 EST

This is an excerpt, extracted by Charlie Hart in IBM Raleigh and appended to the IBM internal NEWSCLIP FORUM, from an article with the above title from the Raleigh News & Observer 1/2/90 (Associated Press):

- * A slice of American history has become as unreadable as Egyptian hieroglyphics before the discovery of the Rosetta stone.
- * More historic, scientific and business data in danger of dissolving into a meaningless jumble of letters, numbers and computer symbols.
- * Americans pay billions to collect the data and may pay millions more to preserve it.
- * Much information from past 30 years stranded on computer tape from primitive or discarded systems unintelligible or soon to be so.
- * Detection of disease, environmental threat or social shift could be delayed because data was lost.
- * Examples:
- 200 reels of 17 year old Public Health Service tapes were destroyed last year because no one could find out what the names and numbers on them meant
- Agent Orange task force unable to use Pentagon's tapes containing date, site, and size of every herbicide bombing in Vietnam.
- Extensive record of U.S. WW II vets exists only on 1600 reels of microfilm of computer punch cards no money or manpower to return data to computer.
- Census data from the 1960s & old NASA data exist only on old tapes some may have decomposed; others may fall apart if run through the balky equipment that survives from that era.
- * Director of National Archives states it would take 25 years to process 20 years of old data if money and manpower existed.
- * One of the biggest headaches is sloppy record keeping no written record of programs or data formats. "Generally it's the last thing you do and pay the least attention to" according to assistant Census director Gerald Cranford.

"Computer Age Causes Key U.S. Data To Be Lost Forever"

jbr@cblph.att.com <j.a.brownlee>

3 Jan 1991 14:43 EST

[text of the same article read by the previous contributor deleted ...]

While the risks of storing important data on media with short life-spans or in undocumented formats are fairly obvious, I suppose that it should not be a surprise that the U.S. government is having such problems. After working at companies that do government work and seeing the many rules in place to "protect" the American taxpayers, this is almost predictable. Because of the procurement process and the length of time it takes to solicit proposals and bids for a system, often by the time the implementation begins, the requirements can be several years old -- a long time for computer systems. Changing requirements to be more reasonable can mean up to a year of red tape. Also, the government has been known to buy some rather non-standard systems.

All in all, this is a rather startling article when you consider the type and amounts of important data that are probably already lost forever.

Joe Brownlee, Analysts International Corp. @ AT&T Network Systems, 471 E Broad St, Suite 1610, Columbus, Ohio 43215; (614) 860-7461 E-mail: jbr@cblph.att.com

Ke: computer "warfare"

John Abolins <jabolins@well.UUCP> Tue, 1 Jan 91 20:41:21 pst

In <u>RISKS-10.70</u>, Sanford Sherizen wrote...

> I would like to gather any *hard* evidence that viruses have been used for > political/military purposes.

> It is possible that the Jerusalem virus was first set off to commemorate a

> Palestinian event but has there been any way to verify this?

The best person to speak for the virus case at Hebrew University in early 1988 would be Y. Radai. In BITNET e-mail "chats" with him in 1988, Radai emphasized that the virus was NOT politically motivated.

Unfortunately, the claim of political origins was circulated in various reports, including an article in the New York Times. The author of the New York Times article had claimed that the Friday May 13, 1988 (when the virus would wreck many files) was connected to May 14, 1988, the 40th anniversary of the establishment of the State of Israel. The author, thus, interpreted May 13, 1988 as the "last day of Palestine". (More correctly, it was the last day of the BRITISH Palestine Mandate.) For the Middle East (where when something goes "boom", many hands reach for a phone to claim the act), it was too "cool". No individual or group claimed credit for this virus. No messages were embedded in the code. The only reason people outside of the Middle East interpreted the virus as a political act was that 1) it was causing problems for an Israeli institution, 2) some computers used by Mossad were allegedly also affected by the virus, and 3) it happened in the Middle East so near Israel's 40th anniversary. By this reasoning, any auto accident or heart attack in Washington, DC must be politically caused. :-)

Sanford Sherizen continues...

> Are there other viruses that have been specifically distributed or > directed to harm a political foe? ...

> Is the virus a potential "small nation's weapon"? Can viruses become

> terrorist surrogates, disrupting an enemy nation without leaving direct

> fingerprints (strings?) traceable back to the ultimate sponsor? What roles

> could viruses play in future small scale intensive conflicts as well as projection ward?

> major wars?

While it is possible that unreported cases with actual political origin exist, the reported substantiated cases of political attacks against computers have been physical, not logical. For example, the bombings of computer facilities in Europe. By these trends, it would look that most computer related attacks will be against the hardware or against the people working with the computers themselves.

I said "by these trends" because there is no guarantee that those trends will hold out forever. The physical means have been favored because they are spectacular, producing fear in the general society, and playing well in the media. Computer "warfare" is more difficult to exploit because to many people the effects of a virus are abstract. (A newscaster try to describe a virus grabs less attention than fire and blood.) But as societies of the West and many other areas of the world become more dependent upon computers, computer may be more enticing targets.

The most enticing aspect of computer targets is the quality of civilization that terrorism most seeks to destroy: trust. (Although many people talk about computer errors and bugs, how many people actual stop using credit cards, ATMs, airlines, etc.?) A savvy group could exploit the computer environment to erode trust in a society's systems. Gumming up the works of financial systems, air traffic controls, etc. could make people uneasy about commerce or travel. It is also possible for a group to attack a very specific types of system (military, government, etc.) for the purpose of incapacitation pure and simple. One of the difficulties in this type of attack is the ability to get a suitable virus on suitable targets. In most cases, it would take someone getting inside (or being able to get an unwitting person to get the code inside). This aspect increases the possibility of detection.

Another possibility is general harassment. Just letting more generalize computer viruses go their way. This mode is hard to detect as evidenced by the difficulty in tracing down virus writers in general. This mode is good for discouraging people from sharing files but, as seen from the past two years of non-political viruses, not all that disruptive. (And even profitable for some software companies. ;-])

Regarding the possibility of viruses as a "small nation's weapon", it does exist. However, similar possibilities exist for other weapons, especially biological. By various reports, a simple biological arsenal (nothing exotic) could be started for much less cost than most aircraft or armored vehicles. Or chemicals, in crude way, could be used. (The old "LSD in the city's water supply" scenario.) Fortunately, for one reason or another (perhaps human inertia), these thing have not yet happened. By the way, making a computer virus can be done by one person. Thus, the usual indicators of offensive development (eg.; satellites photos of installations, movement of materials and personnel, etc.) may be nonexistent. Lest one dismisses the possibility of some Third World group being "smart enough" to produce a computer virus, many terrorist or partisan groups have better educated people than popular stereotypes claim. Also, since a computer virus can be easily transferred on disk, tape, etc., the virus can be produced practically anywhere. And it does not require a member of the group or even sympathetic to it. False flagging is always possible by convincing a technically competent person that the code is being made for another cause, one favored by the person.

With computer technology, an important change occurs in terrorism/partisan warfare: an individual might be able to inflict continuous harm beyond the capabilities of groups using tradition methods. The reason for this is that with groups, the risk of infiltration, defection, disclosure, etc. increase with the number of members. THe advantage of groups is the people resources. But if a terrorist is skilled with certain technologies and chooses to use them, counter measures may be much more difficult.

In my thoughts about such possibilities for computer viruses, I prefer to move away from the usual category of "terrorism" and use the broader category of "partisan conflict". Partisan conflicts can include conflicts not usually considered as warfare or terrorism but, nonetheless could involve computer viruses. Such conflicts could be those involving animal rights, tax protest, abortion, etc. (In short, anything that draws intense conviction and sentiment.)

But in many of these partisan conflicts, computers may be used in generally legitimate applications such as communications services (eg.; BBS's), desktop publishing, etc. In some case, computer "warfare" could occur in the form of using computers to monitor opponents or targets, to increase the effect of black propaganda" and forged materials (eg. fake pamphlets in the name of the target group), possibly to plant misinformation in institutional systems.

Viruses as a terrorist tools might be more attractive to Third World entities on the basis that "blowback" is of less danger than for industrialized entities. That is, entities that don't have computers don't have to worry about the virus affect their systems. Their main problem is the access to the technology to make the virus in the first place.

One of the chief disadvantages with viruses for such warfare is the danger of side effects. For example, indiscriminate disruption of a country's military C3I could lead to firing of weapons in panic with unpredictable results. Also, the disrupted C3I may be part of the same system that is need to give orders for surrender and negotiations. Considering these things, perhaps, a nihilistic partisan group may be more likely to unleash computer viruses. (Just as a group that has no goals and just wants to inflict harm may be more partial to biological agents.)

J. D. Abolins 301 N. Harrison Str. #197 Princeton, NJ 08540 USA jabolins@well.sf.ca.us 609-633-0740

Ke: "Computer Models Leave U.S. Leaders Sure of Victory"

Griffen <griffenj@ncube.com> Mon, 24 Dec 90 11:52:50 PST

In the June-July 1990 issue of Fire & Movement (a wargamer's magazine), there is a _Forum_ section with several articles from various authors regarding battlefield simulation as practiced by the US armed forces.

Probably the most applicable article of these is "The Right Tool Wrongly Used", by Eric M. Walters. In it, he mentions that the simulations and wargames used by the armed forces are regularly modified "in order to achieve training objectives," and not necessarily to promote realism.

He mentions several examples, such as the modification of a rule allowing M60A1 tanks to engage - in force - with enemy vehicles at ranges over 3Km. Walters (Captain in US Marines) states that while hits are possible at those distances, the number of hits in a real war against a "thinking, moving enemy" would be statistically insignificant. The tanker lobby won.

I'll close with the following quote from the article:

...Red Force electronic warfare is reduced or eliminated because its success causes a complete breakdown in exercise force command and control (with a corresponding "loss of staff training time"); and so on. Thus, game "reality" is molded to accommodate Blue Force plans and intentions - not vice versa.

- Jeff

re: "Computer models leave U.S. leaders sure of victory"

David Holland <achilles@pro-angmar.UUCP> Mon, 24 Dec 90 01:57:35 EST

Someone referred to the wargames undertaken by the Japanese prior to the battle of Midway; I quote, from _Miracle_At_Midway_, by Gordon W. Prange, Penguin Books, 1983, ISBN 0 14 00.6814 7:

Ugaki presided with a firm hand, and carried through this grandiose scheme on tabletop with a sunny lack of realism. As he sincerely believed that no situation could exist in which the Japanese would not be in complete control, he allowed nothing to happen which would seriously inconvenience the smooth development of the war games to their predestined conclusion. He did not scruple to override unfavorable rulings of other umpires. (Ch. 4, pg. 31.)

Also:

[Ugaki] cautioned Nagumo that the possibility of an enemy breakthrough must be taken into consideration. Yet Ugaki himself promptly nullified any

good his warning might have done. For during the table maneuvers, the theoretical American forces broke through and bombed Nagumo's carriers while their aircraft were away from their mother ships attacking Midway - the very situation which had concerned Ugaki. Lieutenant Commander Masatake Okumiya, the umpire, ruled that the enemy had scored nine hits, sinking both _Akagi_ and _Kaga_. But Ugaki would not suffer such *lese majeste*, and immediately overruled Okumiya, allowing only three hits, with _Kaga_ sunk and _Akagi_ slightly damaged. And later, when conducting the second phase practice, he blandly resurrected _Kaga_ from her watery grave to participate in the New Caledonia and Fiji invasions. (Ch. 4, pp. 35-6)

Now, considering that all that took place 48 years ago, without any computers, where all the participants could see and understand the workings of the simulation, how much worse will it be in the Pentagon - after all, even if all the generals understand the RISKS of computer simulations, they *still* don't know what algorithms are being used and can't tell if the computer has been engaging in this sort of fudging.

All I can say is I hope they don't have to learn the hard way.

David A. Holland pro-angmar!achilles@alphalpha.com aeneas@blade.mind.org

* re: "Computer models leave U.S. leaders sure of victory"

John C Slimick <slimick@unix.cis.pitt.edu> 26 Dec 90 20:54:09 GMT

The usual reference to the wargaming in the Imperial Navy during the planning of the Midway operation was that on one roll of the dice, the value indicated that the attack force would lose three aircraft carriers. The attack force team immediately appealed to the referee that such an event was impossible. The referee agreed and apparently the next toss was more acceptable. Note: in reality, the attack force lost four carriers.

This is usually cited as an example of the "Victory Disease" that swept over Japan from 1940 through late 1942, where everyone was convinced that the war was won and the Japanese forces were the best (and that's why they won) and so on. My own interpretation is that such games can produce the desired results, and that little has changed since early 1942.

John Slimick, University of Pittsburgh at Bradford slimick@unix.cis.pitt.edu

Ke: "Computer Models Leave U.S. Leaders Sure of Victory"

David Wright <wright@stardent.com> Sat, 29 Dec 90 14:26:28 EST

This discussion caused me to recall the professor in my simulation course, circa 1980. He had consulted for the Army and was extremely skeptical of some of their simulation work. To paraphrase his words, "They use a computer model that runs for a week and then provides a single number as an answer. How can

you possibly have any confidence in that?"

David Wright, Stardent Computer Inc

uunet!stardent!wright

Trojan in MS-DOS 4.01?

John Chapman Flack <76066.1006@compuserve.com> 31 Dec 90 21:06:03 EST

After replacing one SCSI host adapter with another, I found that I was unable to boot my system from my SCSI disk. Knowing that changing host adapters should have no effect on the accessibility of data on a SCSI device, I decided to boot from my original MS-DOS 4.01 distribution diskette (OEMed by AST Research).

I popped the diskette in the drive and hit reset. The system beeped, accessed the diskette, and, without warning or pause, formatted my hard disk. (It ordinarily presents a menu offering to install DOS on a disk or diskette, or to exit to the command level).

After going through the required stages (disbelief, denial, anger, guilt, restoration from backups), I experimented to learn what had happened. When the DOS installation program first gets control, it checks to see if there is a hard disk. If there is a disk, and it has no partition set up (as would be the case with a new system), the familiar menu is presented. If the user chooses to install DOS on the hard disk, the program creates a partition table, and then forces a reboot so the table will be loaded.

If, on bootstrap, the program sees a hard disk which is PARTITIONED but not FORMATTED, it assumes it is continuing the process above. So, without any further interaction with the user, it formats the disk and copies the DOS system files onto it.

Changing the host adapter of course has no effect on the data maintained by the drive and its controller. However, SCSI devices are addressed by logical block number, and the IBM BIOS disk functions use physical cylinder, head, and sector numbers, so each host adapter needs to map the actual logical addresses into fake physical addresses, and different adapters have different algorithms for doing that. The disk, whose fake physical layout appears to have changed (but with data intact), evidently looks to the install program like a partitioned but unformatted disk.

It's easy to see why the installation program was designed as it was. On the other hand, the documentation nowhere mentions that the program might format the disk without consulting the user. (In fact, the only references in the installation instructions to formatting the disk *at all* is an instruction to see the Command Reference manual for information on how to format a disk, and the line "once your hard disk is formatted and partitioned correctly, SELECT completes the installation of MS-DOS...."

So the "feature" meets the definition of a Trojan horse, and in destructive power ranks right up with the biggies (loss of all hard disk data). And it

could have been easily avoided with the addition of "Continue the Install process by formatting the disk (Y/N)?"

Ke: Organizational Aspects of Safety (<u>RISKS-10.71</u>)

Nick Szabo <szabo@sequent.uucp> 28 Dec 90 23:31:53 GMT

Charles Martin proposes the rule, "it costs 1/100th as much to do it right as it costs to do it over."

Often (most of the time?), nobody knows with 100% certainty what is "right". Where knowledge is lacking, and cannot be inexpensively obtained, doing it over -- and over and over again, until it is right -- may be far cheaper and faster than trying to do it right the first time.

Nick Szabo szabo@sequent.com

A RISKy video store kiosk

<r.aminzade@lynx.northeastern.edu> Thu, 3 Jan 91 14:18:15 EST

Last weekend I went to the newly-opened Empire Video store here in Burlington, VT. Empire uses both standard classifications like comedy, sci-fi, foreign, and clever classifications like "feel-good", "tearjerkers" "Bogart", etc. This made it hard to find a film we were looking for. Knowing that most of these stores have a computerized database to help find titles (and show which are currently out), I looked around. sure enough, I found a kiosk with paper catalogs, books of movie reviews, and a CRT aimed out at the floor, clearly for customers. The terminal was off, but we found the ON switch.

"It's broken," said my friend. Sure enough, the machine was displaying only a '>' prompt. Hmm. I tried "DIR". No luck. "Is" didn't work either. Tried several other UNIX, VAX, and DOS commands. EXIT seemed to work! It put me into a menuing system...but it didn't seem to list films, it looked like the entire store-management database!

Before I could stop myself, I had looked up my file information (nothing overdue, can't remember if they had my VISA card number, but I think they did) . I wandered around a bit until I realized that I was doing something not-very-ethical. I turned the machine off before checking which of my neighbors had checked out dirty movies.

Sure Hope the next person to turn on the CRT and try some random commands thinks through the ethical implications. I'll talk to the store manager this week.

Call for papers, VDM '91

Hans Toetenel <winfabi@dutrun.tudelft.nl> 3 Jan 91 14:52:37 GMT

> Call for Papers VDM '91 Formal Software Development Methods Noordwijkerhout, The Netherlands October 21-25, 1991

This symposium is the fourth in a series addressing model-oriented approaches to formal software specification and development. The first three symposia concentrated on specification and design notation and techniques, featuring approaches such as VDM and Z.

The fourth symposium, VDM '91, will concentrate on formal *development*. It will be organised as two days of tutorials and three days of conference, with two parallel tracks throughout: one dedicated to practice, and one dedicated to theory. The symposium will also include tools demonstrations.

After many years of research into and application of model-oriented methods like VDM, Z, RAISE and B, the time is now ripe to record facets of development in more detail, as well as the role of formal development methods in the larger context of problem domain modelling, software engineering, tool development and management. One can identify a spectrum of formality offered or required by various methods, as well as a set of paradigms and principles, such as invent-and-verify, transformation, and design-calculi.

On this basis, papers (to be fully refereed) are welcomed in the following and related areas:

- stepwise development of architectural requirements
- stepwise development of software designs
- development by transformation
- data reification
- rigorous justification
- proof of correctness
- recording of validation and verification conditions
- links between formal development and pragmatic aspects of software engineering (such as requirements tracing, version control, configuration management, change request control, test case generation and validation)
- principles of support tools

Also, project reports , recording industrial experience and ongoing tool development and research are welcomed.

Important dates:	Program Committee
Submission deadline:	Patrick Behm (France)
March 1, 1991	Andrzej Blikle (Poland)
Н	lans Langmaack (Germany)
Notification of acceptance:	Peter Lucas (U.S.A.)
June 17, 1991	Soeren Prehn (chairman) (Denmark)
н	ans Toetenel (The Netherlands)

Camera ready papers due: Jim Woodcock (U.K.) August 16, 1991

Please direct all mail and inquiries to: Hans Toetenel, Delft University of Technology, Faculty of Technical Mathematics and Informatics, PO Box 356, NL-2600 AJ Delft, The Netherlands; E-mail: toet@dutiab.tudelft.nl.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Sat, 5 Jan 1991 12:33:40 PST

An AT&T crew removing an old cable in Newark NJ accidentally severed a fiber-optic cable carrying more than 100,000 calls. Starting at 9:30am on 4 Jan 91, effects included shutdown of the New York Mercantile Exchange, several commodities exchanges, disruption of FAA air-traffic control communication in NY, Washington and Boston, causing lengthy flight delays at those and impinging airports, and blockage of 60% of long-distance telephone calls into and out of

NY, for much of the day. (AP, 5 Jan 91). This came as we approach the anniversary of the 15 Jan 90 nine-hour outage due to a self-propagating bug in the recovery software.

Mathematical Mathematics States And Annalysis And Annalysis Ann

Charles Bryant <ch@dce.ie> Thu, 3 Jan 91 16:56:55 GMT

An article in `The Irish Times' Jan 3 states that extremely sensitive information relating to British military operations in the Gulf may still be on a computer which was stolen from a staff car beloning to Wing Commander David Farquhar on December 17th. The laptop was stolen along with some documents. The documents were later found in a skip, but the computer is still missing.

Presumably the inherent value of the computer made the thief keep it.

Charles Bryant (ch@dce.ie)

[A skip is an open-top container for rubbish (garbage) which is about the size of a small car and is delivered and collected by a special type of vehicle. It must be called something different in the US.] [Dumpster]

Wargames and Reality

<firth@SEI.CMU.EDU> Fri, 4 Jan 91 11:14:00 -0500

I too am concerned at the seemingly naive acceptance by the Department of Defense of the trustworthiness of simulated combat. Others have pointed out that the military cheat at war games, citing especially the Battle of Midway. That is a clear risk. As another example, the German General Staff often gamed the Schlieffen Plan, and also often cheated.

However, there is in my opinion a further, and equally significant risk, even in an honestly conducted simulation, and that is the risk that the simulation incorporate some fallacy critical to the simulated outcome. As an example, consider how, in the 1930s, a possible German invasion of France would be gamed. On the map, the Ardennes would be clearly labelled 'heavily wooded: impassable to tanks', as was the general opinion of the time. A German player who attempted an armoured breakthrough at that point would be immediately stopped by the referee, and informed of his rule violation. But we all know what happenned in 1940.

To relate this to today: the performance figures for military tanks, helicopters, aeroplanes &c are usually taken either from nominal specifications or from the results of field exercises in temperate terrain. However, for the present terrain and climate, values for speed, range, manoeuverability and endurance should be adjusted downwards, by some unknown but probably drastic amount. Has this been done? If so, where did the numbers come from?

Robert Firth

Ke: Vicious elevator door failure recovery (<u>RISKS-10.74</u>)

&om.Lane@G.GP.CS.CMU.EDU> Thu, 3 Jan 1991 21:39-EST

Actually, I believe that elevators with mechanical door sensors (strips) are also programmed to override the sensors and close anyway after a certain number of tries. (I know for sure that the ones in Wean Hall at CMU do this; they are of '60s vintage. They even have the warning buzz you describe.) The reasoning, presumably, is the same as you gave: to defend against sensor failures and denial-of-service attacks.

However, the door closing mechanisms (at least at Wean Hall) are not strong enough to actually hurt a person; in fact they can be forced back by a reasonably determined push. This strikes me as a far better failsafe design than relying on a backup sensor, which is what I think you are advocating. (Think about common-mode failures...) The doors *are* strong enough to be uncomfortable, which I'm sure is deliberate.

Of course, that's not to say that the elevator you encountered is actually designed properly; but the mere use of electrical rather than mechanical sensors does not seem to me to increase the risk in a properly designed system. Mechanical sensors fail, too.

tom lane

...!cs.cmu.edu!tgl tgl%cs.cmu.edu@cmuccvma >internet:tgl@cs.cmu.edu

Ke: Vicious elevator door failure recovery

Mark Brader <msb@sq.com> Fri, 4 Jan 1991 11:52:00 -0500

On some elevators this sensor is not a discrete strip, but is built into the seemingly rigid edge of one of the two layers of door. Either it senses flexing of the edge, or it senses resistance to the door being closed; I can't tell which. It does require more force to operate than the traditional rubber strip, but not so much as to make a "meaningful attempt to crush" the user. Perhaps the elevator in question actually had this type of sensor, but it was not working.

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

Other vicious elevators

Roland G. Ouellette <rouellet@pinnacle.crhc.uiuc.edu> Fri, 4 Jan 91 11:31:15 CST The University of Illinois is suing Otis Elevator because of a pair of these hungry elevators. They've bitten a few people, most notably people pushing computers and/or huge boxes onto and off of the elevator.

Ke: Vicious elevator door failure recovery (Jackson, <u>RISKS-10.74</u>)

jake@mars.bony.com &ake Livni> Fri, 4 Jan 91 14:32:15 EST

Curtis Jackson writes about elevator doors that close, regardless of who's in the way. I know of such elevators, too. (Incidentally, they may use some other sensing mechanism like micro-switches rather than mechanical panels or light beams; an elevator engineer once told me that some elevators use micro-switches in the floor to estimate load and then adjust motor settings accordingly.)

The elevator doors I have seen withdraw several times before becoming insistent, then slowly beep their way closed. This, however, is always followed a few seconds later by a voice on the intercom from a guard downstairs asking if anything is wrong. A human gets into the loop. Guards are always on duty, though I don't know what controls over the elevator they might have from their station.

Jake <AKE@DBCLUA>

Re: Dehumanization by old Cobol programs

Karen Ward <wardk@cse.ogi.edu> Fri, 4 Jan 91 08:59:43 -0800

Darrell D. E. Long writes of thoughtlessly-designed billing software that assumes that all people have only one middle initial. This is not, as he implies, only a risk of old COBOL programs. Instead, he has identified one aspect of a larger ongoing problem: balancing the desire to edit to ensure data validity against the need for sufficient flexibility to accomodate unusual cases. Within the past year alone I have had to argue against system designs that would assume that:

- All names look like "Given I. Family" (I have no middle initial, and my SE has only one name. Many of our customers prefer their family name printed first)
- All children share their parents' family name
- Leading zeros should never print (There are both post-office boxes and street addresses in Portland, Oregon that have significant leading zeros, that is, the same number without the leading zero represents a different address)
- Zipcodes are always 5 (or 9) digits (non-USA zipcodes?)
- Names never contain special characters (Hyphens? Also, some

businesses have exclamation points and numbers in their names)

 All names start with a capital letter followed by lower case (I know of at least one person whose name starts with a lower case and contains an embedded upper case. I know of another whose full name is III, pronounced "three")

For the applications I most frequently work with - business systems for a public utility - I try to keep limiting assumptions about personal information (names, addresses) to a minimum, and to edit with warnings that can be overridden. Our customers will forgive a one-time error far more quickly than they will forgive our inability to correct that error.

Karen Ward (wardk@cse.ogi.edu)

Ke: "Computer Models Leave U.S. Leaders Sure of Victory"

Henry Spencer <henry@zoo.toronto.edu> Fri, 4 Jan 91 21:11:59 GMT

> ...Red Force electronic warfare is reduced or eliminated because its

> success causes a complete breakdown in exercise force command and> control...

After a discussion several years ago on a vaguely similar theme, I had a bit of correspondence with a fellow who'd spent some time in electronic warfare in the Army. (I suspect I should not identify him.) He said that they were normally under severe restrictions in what they could do as part of field exercises, and as a result the folks who were supposed to benefit from said exercises had gotten very blase' about communications practices and the like. Then the EW people, after a lot of begging and pleading, got permission to take the gloves off just once and show the commanders what serious EW could do. His summary of the results: "we paralyzed them".

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

* Re: "Computer Age Causes Key U.S. Data To Be Lost Forever"

Rick Smith <smith@SCTC.COM> Sun, 7 Jan 90 11:18:14 CST

I've been a packrat for most of my life and I've done historical research and I've worked with databases. But I'm finding it very hard to mourn the *general problem* of fading and decomposing magnetic media.

For one thing, the data is meaningless if you don't know how it was collected. NASA has zillions of tapes, but do we really know how all of that data was collected? Which sensor? What setting? Once this information is lost, the data itself is just a tombstone.

For another thing, data has no value for its own sake. If there's a

researcher that can use some of the computer readable data out there, then that's great. But I don't think we should save every last byte "just in case" someone wants to use it in their dissertation on rat populations in rural Podunk. The pot only holds so much. What do we discard instead?

Sure, we should save what is "reasonable." For lack of a better measure, let's save what people will use. For example, we might want to establish a "computer research data recovery fund" which paid the costs for grad students to recover "threatened" digital data and use it in their research. The costs would pay for converting the data to work on the researcher's PC or whatever and for a copy of the data in an archival format. This is somewhat similar to the way that various (usually state) historical societies are making microfilm collections of community newspapers.

I don't know what a good "archival format" would be, however. I read recent descriptions of de-lamination problems with CDs, and I have personal experience with the unreliability of paper tape ...

Rick Arden Hills, Secure Computing Technology Corporation, Minnesota

KE: "Little pitchers have big ears": ATM Risk

<CKAY_MICHAEL@atalla.com [tandem.com?]> 3 Jan 91 16:38:00 +1600

I am currently the sustaining software engineer for the product mentioned by zowie in his posting (11-25-90), and I wanted to clarify some things. He was disturbed by hearing modem tones during an ATM card activation at a Wells Fargo Bank branch. In fact, recording the 300 BAUD transaction (or tapping the phone line) would not reveal his friend's PIN. The PIN is encrypted by the terminal, using DES and a "Unique Key Per Transaction (UKPT)" algorithm (our newer terminals conform to ANSI 9-24, Wells Fargo still uses some older terminals that predate 9-24 with a psuedo UKPT).

Once the transaction is reported to the host, a hardware security box translates the PIN from the terminal's key to some irreversible internal format. Once the PIN is entered into the terminal, it never appears in the clear (that is to say unencrypted) in any computer. This is much better than the usual situation, where you would either be assigned a PIN, or have to write down your PIN and have somebody enter it for you. If anybody would like more details on the process, feel free to contact me.

Michael McKay (MCKAY_MICHAEL @ tandem.com) (408) 435-8850

US MAIL: Atalla, A Tandem Company, 2304 Zanker Road, San Jose, CA 95131

Cars and Automation [again]

&ala.Kumar@IUS3.IUS.CS.CMU.EDU> Fri, 4 Jan 1991 14:18-EST

We were driving at 70 mph [automatic transmission, new car < 1 K miles]. All of a sudden the speedometer cable got cut [I believe] and the needle fell back to 0 mph. In addition there was a heavy noise and could feel the drag on the engine. I pulled out, put it in neutral and raised the engine hood. Nothing wrong with the engine. All other things were OK. Car moved without much problem up to 15 mph. Beyond that it felt like driving at 1st gear. Auto mechanic checked it too. Conclusion:

"Either auto transmission or fuel injection system is taking the input/cue from the speedometer. They think the car is at a lower speed and act accordingly"

Could someone explain the situation?

We could have got into a major accident. Sure, the cause of the accident would have been careless driver.... When I called the rental company for replacement, they could not locate my file on the computer [god knows why] and it took three hours

-balakumar pbk@cs.cmu.edu

[Please respond directly to balakumar, unless this really is a computer-related problem. Otherwise, try the two brothers in Boston on NPR. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Suit says Nissan Fired 2 After reading e-mail

Rodney Hoffman &offman.El_Segundo@Xerox.com> Wed, 9 Jan 1991 07:30:07 PST

Summarized from an article by George White, `Los Angeles Times', 8 Jan 1991

Two former employees of Nissan Motor Corp. USA allege that they lost their jobs after a manager eaves-dropped on their electronic mail messages. Their lawsuit claims that they were illegally discharged and denied their constitutional right to privacy.

The plaintiffs used electronic mail to track the needs of Nissan dealers, occasionally sending personal messages to dealerships. One of the messages was critical of a Nissan manager. The suit mantains that a Nissan manager

intercepted their personal messages and threatened to dismiss the two. One was fired outright, the other was told to resign or be fired. Their attorney said Nissan was retaliating against the pair for filing an invasion of privacy complaint with Nissan's Human Resources Dept. on Dec. 28.

Nissan denies the charges, calling them "unfounded."

Email flash from the past

Paul Eggert <eggert@twinsun.com> Mon, 7 Jan 91 14:01:34 PST

>From <u>RISKS 10.75</u> (7 Jan 91):

Date: Sun, 7 Jan 90 11:18:14 CST [<==== sic ====] From: smith@SCTC.COM (Rick Smith) Subject: Re: "Computer Age Causes Key U.S. Data To Be Lost Forever"

I've been a packrat for most of my life and I've done historical research...

It's ironic that a message about old data claimed to be one year older than it really was. No doubt the problem was a system administrator's error in entering a date after a reboot, the sort of thing that software should warn about but often doesn't. Beware of dates in early January.

[See my Inside Risks column in the January 1991 CACM summarizing some of the more interesting clock problems discussed in the RISKS FORUM over the years (and over the years' ends), albeit familiar to long-time RISKS readers. PGN]

Ke: Cars and Automation: Yes, a computer problem! (<u>RISKS-10.75</u>)

Gregory G. Woodbury <ggw%wolves@cs.duke.edu> Wed, 9 Jan 1991 04:27:34 GMT

This really is a computer related problem. Given that it is a fuel-injection new car, the spark advance and fuel metering are under the control of a micro-controller. On many late model cars, the speedometer readings on the driver's console are derived from the output to the drive wheels (assuming front wheel drive) in the transmission and not from reading the rotation of the wheel!

This is the only source for the micro-controller to know the approximate speed of the vehicle so that it can compute engine load and adjust fuel metering and spark advance.

Additionally, several late models also put the automatic transmission under the control of a micro-controller (usually the same one as is controlling fuel).

The RISKS are obvious. There is only one micro-controller in the system; the car will NOT operate without the controller working properly; there are no redundancies in most of the critical input systems. Additionally, the micro-controllers are overly sensitive in many cases to: changes in voltage

delivered, electromagnetic interference from radio transmissions, electromagnetic interference from power distribution systems, EMI from other systems in the vehicle, and even EMI from traffic sensing devices embedded in the roadways. Further discussion is probably unnecessary.

Gregory G. Woodbury @ The Wolves Den UNIX, Durham NC ggw%wolves@mcnc.mcnc.org UUCP: ...dukcds!wolves!ggw ...mcnc!wolves!ggw

Another train crash in London

"Olivier M.J. Crepin-Leblond" <MEEM37@vaxa.cc.imperial.ac.uk> Wed, 9 Jan 91 13:09 BST

A man has died and 348 people were hurt when a packed rush-hour train failed to stop at Cannon Street station in London, and ploughed into the end buffer.

The train was packed with about 800 commuters. The accident happened on Jan 8th, 1991, at the height of the rush hour, at 8:45am. It appears that the brakes failed to work when the driver tried to slow down when entering the station. The train hit the buffer at the speed of 5 mph only, but some carriages got crushed because of its weight and age. The sixth carriage was pushed onto the fifth carriage. The train was 35-40 years old. The UK's Rail Minister promised a full enquiry. Ambulances, helicopters, and even a London red bus were used to carry the victims to hospital.

Once again there is a major train crash in London. British Rail has had a pretty bad record of crashes. Lately there has been an average of 1 major crash per year. This year it seems that they are reaching their quota pretty early ! The main problem seems to be prolonged lack of investment into new rolling stock, and hence British rail ends up with old trains, old stations, etc. Cost-cutting measures brought more over-crowding during peak rush hours. I have often taken trains similar to the one invollved in yesterday's crash. Most local commuter routes are served using these trains. The ride is something of an experience. During the rush hour, most people stand-up between the seats. Carriages, although being good for natural history museum exhibitions, are crowded to their full load. Yes, carriages with inside walls still made of wood, and grey seats facing each other. The ride is anything but comfortable. One tends to bounce on the seats, as though the train was actually hopping from rail to another rail. 5 years ago British Rail started and extensive refurbishment of these trains. The only visible improvements were are new coat of paint outside, and the replacement of filament light bulbs with fluorescent. Oh, and yes, the logo on the trains was changed from British Rail to Network Southeast. There is no safety mechanism about opening doors. One can open a door whereas the train is in a station or speeding between 2 stations. Some London underground trains have also been built in the 1950's. They should have been replaced 2 years ago, but one of the new replacement trains went off the tracks during trials, and it was all back to the drawing board. London underground says that new trains should be introduced in 1992.

Although there have been so many accidents, I guess I shall miss these British Rail carriages when the new ones replace them (when ? in a year's time I'm told ?). Travelling on Network Southeast was much of an adventurous experience. But like any thrill, it was only good in small doses.

Olivier Crepin-Leblond, Imperial College, London, UK.

Re: NY area fiber-optic telephone cable severed; extensive effects (PGN)

Tony Scandora 708-972-7541 &35048@ANLCMT.CMT.ANL.GOV> Tue, 8 Jan 1991 11:36:49 CST

My father spent all morning Friday 4 January trying to return a phone call from his office near Chicago to a customer in the Dominican Republic. After endless "We're sorry, all circuits are busy. Please try your call later." messages, he heard on the news that a cable had been cut near New York, which affected some overseas calls. He continued trying all day Friday, and never got through. He spent all day Saturday trying to make a FAX call and never got through. A cable cut in Newark made it impossible to place a call from Chicago to the Dominican Republic for at least two full days.

How's that for depending on a single point of failure? It brought back memories of the Hinsdale fire on Mothers Day a couple of years ago, when a fire in an unattended office took out most of Chicago for three weeks. At the time, I started to worry that fifty strategically placed terrorists with street gang incendiaries could cripple the entire country. It could even be done without receiving any return fire. The history of telephone service since then has done nothing to restore my confidence. Back in the bad old days of Ma Bell, they used to brag that the call might be routed through Arizona, Montana, and Guam, but it would get there. Why are today's telecommunications systems designed to depend on extremely vulnerable single points of failure?

Ke: Vicious elevator door failure recovery [<u>RISKS-10.76</u>]

<david@marvin.jpl.oz.au> Tue, 8 Jan 1991 11:04:58 +1100

I speak as an Australian Lift (OZ for "elevator") manufacturer, and so cannot speak directly for USA lifts. However, the observed behaviour is consistent with OZ lifts.

Historically, the door sensors have been a notoriously unreliable element, and whilst many improvements have occured over the years, being at the "working face" of lifts, they still fail regularly. To prevent the lift being out of commision without warrant, controller logic assumes that 4 or 5 retries is good enough if we have stuck people, and then assumes that it must be a sensor failure, and attempts to close. In Oz, this behaviour is often written into building specifications.

However, things are not as bad as they look. Lifts are governed by a VERY large set of regulations, and door related regs are a good part. The door controller design MUST not allow more than a specified force to be applied in the event of a blockage. Whilst this force must be reasonably strong to cover day-to-day events, it is not sufficient to break a limb (130N: let the Regulators beware), although it could cause a broose(?) on the frail. Most door controllers will physically dis-engage the drive mechanism on a solid blockage, allowing even for uncontrolled torque on the closing motor.

"Where the closing of doors is delayed by a period of not less than 10 s through the operation of the passenger-protection device (door beams), the doors may power close with the passenger-protection device in-effective provided that the kinetic energy does not exceed 3.4J, and an audible warning is sounded in the car." Aus. Standards 1735.2 p64

The passenger's main fear is that the doors will close with unreasonable force, to sever the limb; or that the lift will leave the floor with the limb extended thru the door. Above and beyond the controllers S/W checks on timing and sensors, independant door sensors prevent this occurence, all covered by national standards.

Mr Jackson implies that there is a hidden design risk in the behaviour of the doors. Whilst all may not agree on the fine print, it is an area of intense scrutiny and regulation.

These opinions are my own, and although not different to the views of the Company, cannot be taken as an official voice.

David Magnay, Boral Elevators (was: Johns Perry Lifts), 45 Wangara Road, Cheltenham 3192, Victoria, Australia (03) 584-3311 O/seas +61 3 584 3311

KRE: Vicious elevator door failure recovery (RISKS-10.74)

"Olivier M.J. Crepin-Leblond" <MEEM37@vaxa.cc.imperial.ac.uk> Tue, 8 Jan 91 18:24 BST

The few elevators ('lifts' in UK) of the London undergound system are now all operated by computers. They do have a warning beep, and they also have door sensors in case someone gets trapped. The idea has never come into my mind to try to block the doors, but from what I can recall about the commuter crowding during the rush hour, they also shut for good after a few aborted attempts. One can hold them back without trouble.

However the doors of the underground trains are operated by the driver. The only sensor they have checks if the doors are closed or not so that the train cannot start if the doors are not properly shut. About a year ago, one sensor failed and a woman was dragged along the length of a platform. Fortunately other passengers stopped the train by pulling the emergency alarm system.

Once, a friend of mine got his glasses broken when the train door slammed in his face. Drivers are supposed to keep doors open as long as passengers are boarding the train but during the rush hours, they slam them shut so as not to get delayed too much. Again, the doors can be held back, although here if you are not related to Arnold Schwarznegger, it is advisable to request the help from other passengers. So many people have had a bad experience getting trapped in underground train doors !

Personally, I would prefer computers and sensors to control the doors

of any moving carriage. At least when you are trapped the doors open-up again, whereas when there is human interaction, it all depends on his mood.

Olivier M.J. Crepin-Leblond, Elec. Eng. Dept., Imperial College London, UK.

Ke: Vicious elevator door failure recovery

"Michael J. Chinni, SMCAR-CCS-E" <mchinni@PICA.ARMY.MIL> Tue, 8 Jan 91 9:43:50 EST

Given all the comments on this topic I have a question:

Since the elevator door is insisting on closing regardless of something interfering with its closing, what is to prevent the elevator from thinking that the door IS closed and start moving (remember the fact that no button in the elevator was pressed is immaterial since the elevator may be summoned from another floor)?

If there is a final failsafe such that the elevator KNOWS that the door isn't fully closed and therefore that it mustn't start moving then the only concern (albeit a significant one) is the doors closing on a person. Seriousness of this depends upon the force the door exerts on the object blocking its full closing.

If there ISN'T such a failsafe then this problem is a fatality (and a gruesome fatality) waiting to happen.

Michael J. Chinni US Army Armament Research, Development, and Engineering Center Picatinny Arsenal, New Jersey ARPA: mchinni@pica.army.mil UUCP: ...!uunet!pica.army.mil!mchinni

Ke: Vicious Elevators

Russell McFatter <russ@alliant.com> Tue, 8 Jan 91 10:02:49 EST

All of the elevators I've seen have some kind of door-edge safety device--(officially called a "safety edge"). The older (and still most prevalent) style is the mechanical rubber bumper, which usually has to be pushed in by 1-2 inches to cause the door to retreat. Other elevators have a thin plastic (but still mechanical) edge which works much the same way. The newest Otis installations I've seen all have a proximity sensor, which is a plastic device mounted flush with the inner door (and usually has a small calibration light)-most of the time, these reverse the door before it touches anything. In an event where it doesn't (such as when the OUTER door is blocked), you are protected by devices which limit the force that the door can apply. Both the closing speed (feet per minute) and closing force (pounds) of an elevator door are regulated by law (and is one of those things that should be checked when an elevator is inspected). Rather than a clutch, I believe that most modern elevators limit the closing force of the door electronically. The test is to resist the door WITHOUT tripping the safety edge or "electric eyes" (on elevators equipped with this). It's usually firm, but shouldn't be able to crush or otherwise injure someone. Most importantly, the elevator should not move with an obstruction in the door, even if the door is refusing to reopen. This is one place where I think that advanced technology has reduced RISKs to the public; modern elevators can detect "unreasonable" situations that mechanical controllers don't (such as: door does not close within a certain time limit), and take appropriate action.

The safer we make something (elevator doors), the more people take this safety for granted, and, ironically, we end up with more types of unpredictable trouble. I've always been amused by the New York public service commercials which advertise the hazards of subway-train doors, and makes the point that "these doors mean business" and do not reopen (at one point, showing them with teeth). People know to stay out of the way, and this helps to avoid accidents. Imagine what would happen if you tried to introduce the first subway system based on the design that exists in most modern cities (including the very modern Washington D.C. "metro"): A crowded concrete platform ends at a five-foot drop to the tracks below; no walls or doors to prevent people from falling (or being shoved) off the edge; and no way back up once one falls. At the bottom are exposed metal rails carrying lethal voltages at huge currents. Whether or not one survives, the next train arriving at the station won't be able to stop in time to avoid hitting him. Even those passengers who remain on the platform and successfully board a train, avoiding those nasty teeth-bearing doors, will find themselves sitting or standing(!) in a boxful of glass windows, doors, metal rails, and with nothing particular to keep them in place when the train derails or smashes into another train, filling the dark tunnel with toxic smoke. Would you expect this design to be approved?

Still, the greatest RISK to your health isn't the subway itself, but other passengers (especially in NYC).

--- Russ McFatter [russ@alliant.Alliant.COM]

✓ call-for-papers, Journal of Computer Security

Sushil Jajodia <jajodia@gmuvax2.gmu.edu> Tue, 8 Jan 91 09:27:01 -0500

> CALL FOR PAPERS JOURNAL OF COMPUTER SECURITY

The Journal of Computer Security is a new archival research journal on computer security, to be published quarterly by IOS Press, Amsterdam. It will publish significant advances in the theory, architecture, design, implementation, analysis, and application of secure computer systems. Its scope encompasses all aspects of computer security, including confidentiality, integrity, and denial of service. Subject areas include computer architecture, operating systems, database systems, networks, distributed systems, formal models, verification, algorithms, mechanisms, and policies.

Editors-in-Chief:

Prof. Sushil JajodiaDr. Jonathan MillenGeorge Mason UniversityThe MITRE CorporationDepartment of Information SystemsMail Stop K325and Systems EngineeringBurlington RoadFairfax, VA 22030-4444, U.S.A.Bedford, MA 01730, U.S.A.jajodia@gmuvax2.gmu.edujkm@mbunix.mitre.org(703) 764-6192(617) 271-3580

Editorial Board Includes:

Marshall Abrams, MITRECarl Landwehr, NRLThomas Beth, U. of KarlsruheE. Stewart Lee, U. of TorontoMatt Bishop, DartmouthTeresa Lunt, SRIJohn Dobson, Newcastle upon TyneJohn McLean, NRLGerard Eizenberg, ONERA/CERTRavi Sandhu, George MasonVirgil Gligor, U. MarylandMarv Schaefer, TISBhavani Thuraisingham, MITRECarl Landwehr, NRL

Instructions to Authors:

Submit six copies of your manuscript to one of the editors-in-chief with a submittal letter signed by one of the authors. In case of multiple authors, designate an author for correspondence. Please keep the editors informed of any changes of address.

Submitted papers must be original and present a significant result, and must not have been previously published or submitted for publication elsewhere, although portions may have been published in conference proceedings. It will be assumed that all necessary clearances for publication have been obtained by the author(s) by the time a paper is submitted for publication.

Papers will be refereed in a manner customary with scientific journals before being accepted for publication.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



David A Smallberg <das@CS.UCLA.EDU> Fri, 11 Jan 91 11:54:34 PST

Summarized from an article by Roxana Kopetman, Los Angeles Times, 10 Jan 1991:

Long Beach, California, police officials believe that a programming error partly explains why their department has the worst crime solving record among 11 large California cities.

The California Department of Justice ranks departments by their rate of solving

crimes. Long Beach has placed last 11 times in the last 15 years. Last year, for example, the city solved 14.2% of its cases; the statewide average is 22%.

However, the department just found out that their system lists a crime as solved only if it is solved in the same month it was reported. Other police departments don't do this. The tallies are done by a program in the city's information services bureau.

Police don't put all the blame on the program. They cite an understaffed detective bureau and officers taking time off for job-related injuries at a rate three times the state average, taking twice as long as average to return to work.

-- David Smallberg, das@cs.ucla.edu

✓ Unusual distance metric could waste consumers' time and gas

David A Smallberg <das@CS.UCLA.EDU> Fri, 11 Jan 91 13:00:23 PST

A friend related an experience he had calling a swimming pool supply company's 800 number to find a local distributor. The operator asked for his zip code and told him the address of the nearest distributor, saying it was 3.5 miles away. It actually was more like 8 miles, so my friend figured the distance was measured from his post office. Since he lives near a zip code boundary, he asked for the nearest distributor from the neighboring zip code, hoping to find something closer. This is where things started to get weird, so he tried zip codes from his office and parents' home:

Start location & ZipNearest distributor location & distanceSherman Oaks, CA 91423Reseda (3.5 reported miles, 8 actual miles)North Hollywood 91607Hacienda Heights (30 miles! Reseda's closer!)Santa Monica90405Torrance (15 miles)West Los Angeles 90064Carson City, Nevada (400 miles!)

At this point my friend figured out what was happening:

Sherman Oaks 91423 ==> 91335 Reseda North Hollywood 91607 ==> 917xx Hacienda Heights Santa Monica 90405 ==> 905xx Torrance West Los Angeles 90064 ==> 897xx Carson City, Nevada

The programmer obviously assumed that proximity in zip codes meant proximity in space. E.g., for 90064, since there was no distributor in 900xx, the program tried 901xx and 899xx, then 902xx and 898xx, etc. How many customers wasted their time and gas going to the wrong store? How much business did the company lose from people who decided not to make a long trip?

I've noticed similar foolishness from companies that assume that any store location in my telephone area code (818) is worth telling me about, while none of the nearer stores in neighboring 213 are. -- David Smallberg, das@cs.ucla.edu

Computers Stolen in the USSR

Sanford Sherizen <0003965782@mcimail.com> Thu, 10 Jan 91 21:01 GMT

The following falls into the "Isn't this a small world" category. It appears that the Soviet Union is getting more Westernized by the moment. Their criminals and police seem to be just like ours.

The message originally appeared on internet news and then was posted on a net concerned with Soviet computing (USSRECOM).

Sandy

In article <1991Jan7.150851.2143@hq.demos.su>, avg@hq.demos.su (Vadim Antonov) writes:

|> Hi, our small team just faced to a new problem: some thieves

|> stole our net's major backbone machine (a 486 :-). These guys are

> already caught but the machine is still a "material evidence" and

|> we had to switch to (much heavier :-) VAX. Is it a first actual

|> case of stealing of a backbone hardware? :-) :-) At least we found

> that all the messages were stolen together with the machine :-).

|>

> Vadim Antonov

|> DEMOS, Moscow, USSR

Ke: British military information stolen (Bryant, <u>RISKS-10.75</u>)

Stephen Carter <stevedc@syma.sussex.ac.uk> Thu, 10 Jan 91 18:14:17 GMT

> An article in `The Irish Times' Jan 3 states that extremely sensitive
> information relating to British military operations in the Gulf may
> still be on a computer which was stolen from a staff car ...

It is worth adding that this information was known and published outside of the UK, but was not published (censorship) in the UK until (I think) 6 Jan 91 when Associated Press threatened to run the story anyway.

Stephen Carter, The University of Sussex, Falmer, Brighton BN1 9RH, UK Tel: +44 273 678203 Fax: +44 273 678335 UUCP: stevedc@syma.uucp

✓ Vicious Subway Cars (was: Vicious Elevators)

Unix Guru-in-Training <elr%trintex@uunet.UU.NET> Thu, 10 Jan 91 12:42:54 EST Here's a quick rundown on RISKS of stepping through the doors on a New York City subway car: each of the twin doors can be as much as 3 inches open when the train starts moving, giving you a maximum gap of 6". Although an interlock prevents the train from starting while the doors are open (called the "indication" by the train crew), the sensors aren't too precise. People can (and do) get dragged by moving cars when they're stuck in the doors. Usually it's their own fault -- hyped up New Yorkers who won't wait the next three or five minutes for the next rush hour train (or ten or twenty minutes off peak) blocking the doors open in the vain hope the conductor will re-open and let them in. As a previous RISK poster noted, this all depends on the conductor's mood and if s/he is in a hurry or not. It also depends on their line supervisors: some managers emphasize speed, others passenger safety.

A few years ago the Transit Authority had a problem with "doors opening enroute" on the older (pre-1976 or so) cars -- an individual door would open while the train was in motion, once on a speeding express train (thankfully, no one was hurt). The TA rewired all their newer trains with an interlock so that the emergency brake would activate if the doors opened while the train was in motion.

You can experiment with this safety interlock by attempting to force one of the doors open while the train is moving. One day I observed two teenagers on the way to Brooklyn doing exactly that, thrilling over pushing open a door two inches as the train sped through the tunnel. When I warned them that they would kick in the emergency brake if they went too far they had a spell of enlightened self-interest (it can take ten or fifteen minutes for the crew to reset the emergency brake) and left the poor door alone.

Ed Ravin, Prodigy Services Company, White Plains, NY 10601 elr@trintex.UUCP +1-914-993-4737 philabs!trintex!elr

Vicious Doors on London Underground/Network South-East

Pete Mellor <pm@cs.city.ac.uk> Thu, 10 Jan 91 21:33:56 PST

I was interested in Olivier M.J. Crepin-Leblond's two mailings (<u>RISKS-10.75</u>) regarding the recent train crash and the behaviour of tube train doors.

I am also a victim (sorry, commuter! :-) of "Network South-East", the bit of what used to be British Rail that serves East Anglia and the area south-east of London. They are a by-word for discomfort and overcrowding, even where the rolling stock is new, as it is on the lines from Peterborough and Cambridge into London King's Cross. It was recognised at the enquiry into the Clapham rail disaster that a large proportion of the deaths and serious injuries in a crash can be attributed to passengers having to stand in the aisles between the seats. Even a low-speed impact means that standing passengers who insist on obeying Newton's first law of motion will continue their journey along the carriage until brought to rest by their fellow passengers or by the door to the adjoining carriage.

Even so, it does not appear to be cost-effective to supply adequate numbers
of carriages to cope with the rush-hour. After all, the management has to show a profit so that privatisation will attract investors, and a yearly season ticket between Stevenage and London only costs 1744 pounds sterling.

Another bit of cost-cutting is to use driver-only trains. There is no guard to check the doors before the train pulls out. This is so on most rail and underground services. There is usually a TV monitor which the driver can use to check the length of the platform. This does not seem to be particularly effective, judging by the number of incidents I have personally witnessed over the last few years, such as:

A driver closing the automatic doors and pulling away after a mother got out but before her children had time to leave the train. (Frantic waving and shouting by other people on the platform made him stop.) - Network South-East.

An elderly woman boards the train (Underground: Piccadilly Line), and the driver closes the doors and moves off before her equally elderly husband can get on.

I leaped onto a crowded tube train (Underground: Metropolitan Line) carrying a shoulder bag just as the doors were closing. I got on, but my bag didn't. The doors closed around the strap, and the train moved away with the bag hanging outside the carriage, and me pinned to the door by the strap around my shoulder, just waiting for the first obstruction to snag the bag. Fortunately, someone pulled the emergency handle, and the train stopped before it entered the tunnel.

What has this got to do with computers? Not a lot! All these incidents occurred with a human in the loop (just one human, and obviously not very firmly in the loop!). I think that less, not more, automation is the answer to safety here. Bring back the guard!

(I went through King's Cross on the Circle Line while the fire was raging a few years ago. They're gonna get me one day! :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

✓ Defence of British Rail/Network SouthEast

David Green (MSc 90/91) <davidg@aipna.edinburgh.ac.uk> Fri, 11 Jan 91 15:33:24 GMT

In the latest RISKS DIGEST:

Date: Wed, 9 Jan 91 13:09 BST From: "Olivier M.J. Crepin-Leblond" <MEEM37@vaxa.cc.imperial.ac.uk> Subject: Another train crash in London

> [general criticism of British Rail esp. Network SouthEast]

Yes, there's been a major train crash in London. But I've seen no claims that computers were involved - as Olivier points out, BR's main problem is hardware

dating from the 1950's, and hardly the over-enthusiastic application of new technology. The UK news reports I heard only listed 1 fatality, and I wouldn't like to estimate the number of deaths that would be likely to result from all of the rail commuters driving into London instead. For seven years I travelled about 20 miles a day (going to and from school) by Network SouthEast, and although we didn't always get seats, clean trains, or particularly punctual arrivals, we always got there in one piece. I don't think there exists a perfect public transport system; the UK rail network only offers one of the better alternatives.

Unlikely though this may seem to some of your readers, I am in no way connected to British Rail, Network SouthEast, or any of their subsidiaries.

David Green

RISKS of computer-assisted emergency dispatch systems

Unix Guru-in-Training <elr%trintex@uunet.UU.NET> Thu, 10 Jan 91 13:08:34 EST

Thanks to budget cuts a fire company was recently closed near Richmond Hill, in Queens (New York City). This past Monday, two people died in a fire nine blocks from the closed engine company. It's been getting lots of local news coverage, because the firefighter's union, in a bid to reverse the closures, has claimed that those persons might have lived if the engine company had not been shut down.

In the post-mortem analysis of the response to the fire, several other problems were turned up that cost time in getting water pumped into the burning building. The biggest one was that the engine company that was dispatched (engine companies have the pumps and hoses that will squirt water from a hydrant into the fire, ladder companies have the rescue team for clambering into the building and recovering people stuck inside) was told that they were the "auxiliary" engine company. So they did what an auxilliary company is supposed to do, namely hook up to the second-closest hydrant and let the "main" company get the first assault into the fire. But the "main" company was supposed to be the engine that had been closed down, and so no other water-pumping equipment was sent. The firefighters quickly realized the mistake, and lost only a couple of minutes putting back their hoses and moving to the closer hydrant.

Apparently the Fire Department's computer dispatch system was not updated about the demise of the engine company, and thus designated the remaining engine in the area as the auxiliary. And despite news headlines about firehouse closings, none of the dispatchers realized in time that they were making an error.

It looks like the people who build dispatch systems (or telephone operator's consoles, airline reservation systems, etc) are interesting only in improving "efficiency", which usually translates to less operators and lesser-trained operators. In a place like NYC, without computer assistance dispatchers would have to be well versed in the operations of the emergency service they were controlling, if not the local neighborhood their units were operating in. Now, from what I've heard over my scanner, dispatchers can be almost anyone who can sit in front of the computer console that's supposedly keeping track of which units are where and which calls from 911 haven't been answered yet. Operators can be changed or transferred frequently because the computer is supposed to "remember" the status of all outstanding calls. So more work is dumped on lesser-trained people, and the results are degraded service and mistakes like that described above. (To be fair, this is less true of the NYC Fire Department than of the Police Department.)

Ed Ravin, Prodigy Services Company, White Plains, NY 10601 elr@trintex.UUCP +1-914-993-4737 philabs!trintex!elr

Znd IFIP Dependable Computing Conf.

Rick Schlichting <rick@cs.arizona.edu> 11 Jan 91 18:17:06 GMT

[Please note that the preregistration and hotel reservation deadlines are fast approaching.]

*** Final Call for Registration *** Second IFIP Working Conference on

DEPENDABLE COMPUTING FOR CRITICAL APPLICATIONS Can we rely on computers?

Hotel Park Tucson, Tucson, Arizona, USA February 18-20, 1991

Organized by IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance

Registration Information:

Advance registration is strongly encouraged. The advance registration fee, due by January 15, is 300 U.S. dollars, by bank draft drawn on a U.S. Bank. Limited on-site registration will be available at a cost of 340 U.S. dollars.

The registration fee includes: attendance at the Working Conference, a welcome reception, 3 lunches, coffee breaks, and the banquet, as well as one copy of the conference pre-prints and a copy of the proceedings. The proceedings will be published as a volume of the Springer-Verlag series "Dependable Computing and Fault-Tolerant Systems."

CONFERENCE REGISTRATION FORM

Return to: R. D. Schlichting, 2nd DCCA Working Conference, Dept. of Computer Science, University of Arizona, Tucson, AZ 85721

Name:

Affiliation
Address:
Phone:
email:
Registration Fee:
Advance Registration \$ 300
(Must be received by Jan. 15)
Regular Registration \$ 340
Ticket to Reception and Banquet
for guests (\$60 per person)
ΤΟΤΑΙ
Payment must be made in U.S. Dollars, by bank draft drawn on a U.S. bank.
Accommodations for the Working Conference will be provided by the Hotel Park
Tucson. Attendees should make their reservations prior to January 17 either by
mailing in the form below or telephoning the hotel. The hotel can be reached
from the Tucson airport via rental car, taxi, or van. Van service is provided
by the Arizona Stagecoach, at a cost of \$7.50 each direction. To make use of
this service, exit the airport to the curb and look for a van with "Arizona
Stagecoach" printed on the side. No reservations are necessary.
HOTEL REGISTRATION FORM
2nd IFIP Working Conf. on Dependable Computing for
Critical Applications (February 18-20, 1991)
Return to: Hotel Park Tucson, 5151 E. Grant Road, Tucson, AZ 85712
Phone: 1 (602) 323-6262 or 1 (800) 257-7275
Please reserve accommodations for:
Name:
Address:
Smoking (Yes/No):
Will Share Room With:
Arrival Date: Time:
Departure Date: Time:
Telephone:
Check in time is 2:00 nm. Check out is 12 noon. Reconnections must be received
by Japuary 17 to insure rate. Rooms will be held until 6:00 n m. on the date
of arrival. To guarantee your reservation, please enclose a check for one
night's deposit or assure your reservation, please enclose a check for one
Express, VISA, Mastercard, Carte Blanche).
, , , ,,
Card Type: Exp. Date:

Card #:	
Signature	::

Rates:	# rooms # people
Suite (One Bed)	\$85

Suite (Two Beds) \$85

Suite accommodations are on a space availability basis. All reservations subject to sales and occupancy taxes.

For More Information:

Rick SchlichtingBill SandersGeneral ChairLocal Arrangements ChairDept. of Computer ScienceDept. of Elect. and Comp. Engin.University of ArizonaUniversity of ArizonaTucson, AZ 85721 USATucson, AZ 85721 USA

 Voice: 1 (602) 621-4324
 Voice: 1 (602) 621-6181

 FAX: 1 (602) 621-4246
 FAX: 1 (602) 621-8076

 email: rick@cs.arizona.edu
 email: whs@ece.arizona.edu

FIRST CONFERENCE ON COMPUTERS, FREEDOM & PRIVACY

Dorothy Denning <denning@src.dec.com> 10 Jan 1991 1519-PST (Thursday)

Please copy, post & circulate! [Abridged by PGN. Send EMAIL to jwarren@well.sf.ca.us for more info.]

Pursuing Policies for the Information Age in the Bicentennial Year of the Bill of Rights

Tutorials & Invitational Conference, Limited to 600 Participants Monday-Thursday, March 25-28, 1991

Airport SFO Marriott Hotel, Burlingame, California (San Francisco Peninsula)

Co-sponsors & cooperating organizations include Institute of Electrical and Electronics Engineers-USA Association for Computing Machinery **Electronic Networking Association** Electronic Frontier Foundation Videotex Industry Association Cato Institute American Civil Liberties Union ACM Special Interest Group on Software **IEEE-USA Intellectual Property Committee** ACM Special Interest Group on Computers and Society ACM Committee on Scientific Freedom and Human Rights IEEE-USA Committee on Communications and Information Policy The WELL Portal Communications Autodesk, Inc.

Sponsored by the Computer Professionals for Social Responsibility A nonprofit educational corporation (415)322-3778, e-mail: cfp@well.sf.ca.us. fax: (415)851-2814

ABOUT COMPUTERS, FREEDOM & PRIVACY

We are at a crossroads as individuals, organizations and governments depend more and more on computers and computer networks. Within ten years, most global information will be collected and utilized electronically.

The 1990's are the pivotal decade in which statutes, policies and judicial precedents will be developed for controlling access, use -- and abuse -- of computerized information and electronic mail.

Current government and private-sector policies are an uncoordinated jumble, created as each group evolves ways to collect, manipulate, extract, share and protect computerized and networked information and services.

Data on individuals and groups is being computerized by numerous agencies, organizations and special interests, often without the knowledge or approval of those it concerns, and with varying degrees of accuracy.

Computers can greatly assist individuals, organizations and government in making sound decisions based on efficient access to adequate information -- for personal benefit, business improvement and national well-being.

Or, inappropriate use and regulation can seriously threaten fundamental freedoms, personal privacy, and the democratic processes that are at the very foundation of this nation and of any free society.

ABOUT THE CONFERENCE SESSIONS (Tuesday-Thursday, March 26th-28th)

PLENARY SPEAKERS:

* Laurence H. Tribe, Professor of Constitutional Law, Harvard Law School, offering major policy proposals in the opening Conference session, "The Constitution in Cyberspace: Law & Liberty Beyond the Electronic Frontier".

* Eli M. Noam, Director of the Center for Telecommunications and Information Studies, Columbia University, and a recognized leader in telecommunications regulation, international communications policies and economics, will discuss, "Network Environments of the Future: Reconciling Free Speech and Freedom of Association."

* William A. Bayse, Assistant Director, FBI Technical Services Division, Washington DC, providing perspectives on "Balancing Computer Security Capabilities with Privacy and Integrity" at the Wednesday evening banquet.

THE CONFERENCE SESSIONS offer diverse speakers & panel discussions:

Trends in Computers & Networks. Overview and prognosis of computing capabilities and networking as they impact personal privacy, confidentiality, security, one-to-one & many-to-one communications, and access to information about government, business and society.

International Perspectives & Impacts. Other nations' models for protecting personal information and communications, and granting access to government

information; existing and developing laws; requirements for trans-national dataflow and their implications; impacts on personal expression; accountability.

Personal Information & Privacy. Government and private collection, sharing, marketing, verification, use, protection of, access to and responsibility for personal data, including buying patterns, viewing habits, lifestyle, work, health, school, census, voter, tax, financial and consumer information.

Law Enforcement Practices & Problems. Issues relating to investigation, prosecution, due process and deterring computer crimes, now and in the future; use of computers to aid law enforcement.

Law Enforcement & Civil Liberties. Interaction of computer crime, law enforcement and civil liberties; issues of search, seizure and sanctions, especially as applied to shared or networked information, software and equipment.

Legislation & Regulation. Legislative and regulatory roles in protecting privacy and insuring access; legal problems posed by computing and computer networks; approaches to improving related government processes.

Computer-based Surveillance of Individuals. Monitoring electronic-mail, public & private teleconferences, electronic bulletin boards, publications and subscribers; monitoring individuals, work performance, buying habits and lifestyles.

Electronic Speech, Press & Assembly. Freedoms and responsibilities regarding electronic speech, public and private electronic assembly, electronic publishing, prior restraint and chilling effects of monitoring.

Access to Government Information. Implementing individual and corporate access to federal, state & local information about communities, corporations, legislation, administration, the courts and public figures; allowing access while protecting confidentiality.

Ethics & Education. Ethical principles for individuals, system administrators, organizations, corporations and government; copying of data, copying of software, distributing confidential information; relations to computer education and computer law.

Where Do We Go From Here? [closing session] Perspectives, recommendations and commitments of participants from the major interest groups, proposed next steps to protect personal privacy, protect fundamental freedoms and encourage responsible policies and action.

Also: Tuesday and Wednesday will include structured opportunities for attendees to identify groups with whom they want to establish contact and, if they wish, announce topics they would like to discuss, one on one.

ABOUT THIS PREMIER EVENT

This is an intensive, multi-disciplinary survey Conference for those concerned

with computing, teleconferencing, electronic mail, computerized personal information, direct marketing information, government data, etc. -- and those concerned with computer-related legislation, regulation, computer security, law enforcement and national and international policies that impact civil liberties, responsible exercise of freedom and equitable protection of privacy in this global Information Age.

For the first time, this four-day invitational event will bring together representatives from all of these groups and more, all in one place, all at one time.

Many of the recognized leaders and strongest advocates representing the various groups having an interest in the issues of the conference will discuss their concerns and proposals.

A maximum of 600 applicants will be invited to attend. Balanced representation from the diverse groups interested in these issues is being encouraged. Please see the enclosed Invitation Application for details.

To inform participants about topics beyond their specialties, half-day seminars are scheduled for the first day (Monday, March 25th). These parallel tutorials will explore relevant issues in computing, networking, civil liberties, regulation, the law and law enforcement. Each tutorial is designed for those who are experienced in one area, but are less knowledgeable in the subject of that tutorial.

To explore the interactions and ramifications of the issues, conference talks and panel discussions are scheduled for the remaining three days (Tuesday-Thursday, March 26th-28th). These will emphasize balanced representation of all major views, especially including probing questions and discussion.

Explicit Conference events to foster communication across disciplines are planned. Working luncheons, major breaks and two evening banquets will further encourage individual and small-group discussions.

Speakers include (among others) Ken Allen, Sharon Beckman, Jerry Berman, Paul Bernstein, Sally Bowman, David Burnham, Mary Culnan, Peter Denning, Dorothy Denning, Dave Farber (UPenn), Cliff Figallo, David Flaherty, John Ford, Bob Gellman, Janlori Goldman, Harry Hammit, Martin Hellman, Evan Hendricks, Lance Hoffman, Don Ingraham, Bob Jacobson, Mitch Kapor, Tom Mandel, John McMullen, Peter Neumann, Donn Parker, Ron Plesser, John Quarterman, Jack Rickard, Tom Riley, Lance Rose, Marc Rotenberg, Noel Shipman, Harvey Silverglate, Gail Thackeray, Robert Veeder, Willis Ware, Sheldon Zenner.

ABOUT THE LOW-COST TUTORIALS (Monday, March 25th)

Seminars on the first day offer introductions to the different disciplines that intersect in this conference. These are surveys for individuals not already expert in the topics presented. These half-day tutorials are scheduled in four parallel tracks:

Global Communications & the Worldwide Computer Matrix. [morning*] Survey of electronic-mail & teleconferencing services, global information access, remote services and the matrix of networks.

Low-Cost Computer Networking & Computer Bulletin Board Systems. [afternoon*] Reviews e-mail, bulletin board and teleconferencing alternatives on personal computers; outlines low-cost PC-based networks and their gateways to the global matrix.

-- Mark Graham*, co-founder of Institute for Global Communications, PeaceNet and EcoNet; Pandora Systems

Current & Proposed International Policies. [morning*] Law and regulation that will or may impact trans-border data-flow and computer communications, impacting U.S. information practices and international business.

Federal Legislation Impacting Computer Use. [afternoon*] Detailed review of landmark federal statutes impacting access to information, privacy of information, computer security and computer crime. -- Marc Rotenberg*, former congressional counsel and expert on federal legislation, CPSR, Washington DC.

How Computer Crackers Crack! [morning*]

Suggested by a deputy district attorney specializing in high-tech crime, this is for law enforcement officials, prosecutors, systems administrators and Bulletin Board System (BBS) sysops.

-- Russell Brand*, computer security specialist; programmer with Reasoning Systems, Palo Alto CA.

How Computer Crime is Investigated.

[afternoon*] This reviews investigation, search, seizure and evidence requirements for pursuing computer crime. It is for computer users, computer owners, BBS sysops and investigators unfamiliar with computer crime practices.

Information Security. [afternoon*]

Survey for systems managers of internal and external threats, security measures, alternatives and other computer and data security issues. -- Donn Parker*, a leading consultant in information security and computer crime, SRI International.

* - Lecturers, descriptions and times were confirmed as of 1/8/91, but may be subject to change.

CONFERENCE CHAIR

Jim Warren, Autodesk, Inc. & *MicroTimes* 415-851-7075, jwarren@well.sf.ca.us / e-mail

= Request for Invitation =

First Conference on Computers, Freedom & Privacy March 25-28, 1991

Monday: Tutorials, Tuesday-Thursday: Conference Sessions SFO Marriott Hotel, 1800 Old Bayshore Hwy., Burlingame CA 94010 For hotel reservations at Conference rates, call: (800)228-9290 #3

** Invitational Conference, limited to 600 participants. **

To facilitate useful dialogue and balanced participation by representatives from all of the diverse groups interested in these issues, attendance is limited. (The capacity of the Conference facility is similarly limited).

All interested individuals are encouraged to request an invitation. Invitations will be primarily issued on a first-come, first-served basis within each major interest group.

Fees if payment is received:by Jan.31Feb.1-Mar.15after Mar.15Tutorials (full day)\$ 95\$ 145\$ 195Conference (3 days)\$ 295\$ 350\$ 400Conference Registration fee includes three luncheons, two banquet meetingsand selected handouts:Please make checks payable to "Computers, Freedom & Privacy/CPSR".

Please don't send cash. Invitations will be promptly issued, or the uncashed check will be voided and promptly returned.

Please type or print. Thank ye, kindly. name: title: organization: mailing address: city, state ZIP: phone(s): fax: e-mail:

Comments to assist in evaluating this request:

To aid in balancing participation among groups,

please check all significantly applicable items.

- [] user of computers or computer networking
- [] user of electronic-mail services
- [] user of teleconferencing services
- [] user of direct marketing services
- [] user of computerized personal information
- [] user of government information
- [] computer professional
- [] BBS sysop (bulletin board system operator)
- [] systems administrator / infosystems manager
- [] network administrator
- [] computer / communications security specialist
- [] provider of data communications services
- [] provider of electronic-mail services
- [] provider of teleconferencing services
- [] provider of direct marketing services
- [] provider of computerized personal information
- [] provider of government information
- [] legislative official [] federal [] state
- [] regulatory official or staff [] federal [] state
- [] law enforcement official [] federal [] state [] local

<pre>[] prosecutor [] federal [] state [] local [] judicial representative [] federal [] state [] local [] criminal defense attorney [] corporate or litigation attorney [] civil liberties specialist [] journalist [] newspaper [] television [] radio [] other [] other: [] other: <<1/7/91<></pre>		
Please mail form and payment to: CFP Conference, 345 Swett Road, Woodside CA 94062 Privacy Notice: This information will not be sold, rented, loaned, exchanged or used for any purpose other than official CPSR activity. CPSR may elect to send information about other activities, but such mailings will always originate with CPSR.		
Sponsor: Computer Professionals for Social Responsibility, (415)322-3778 A nonprofit, educational corporation [Internal Revenue Code 501(c)(3)] e-mail: cfp@well.sf.ca.us; fax: (415)851-2814 Chair: Jim Warren, (415)851-7075		
Search RISKS using <u>swish-e</u>		

Report problems with the web pages to the maintainer



// (No) Viruses in Iraq's EXOCET? (Misguided Missiles)

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 15 Jan 91 11:10 GMT+0100

French press (La Liberation) and media reported (Jan.10) in some detail that computer viruses could be planted, either in advance or afterwards, in French EXOCET rockets to influence their performance such as to misguide them. Following a report of the German Press Agency (dpa), German media (on Jan.11) were full of reports about "viruses in Hussein's rockets". According to dpa, (unnamed) French computer scientists said:

- manufacturers of war material usually implant, "for mere commercial reasons", viruses in exported war electronics to provoke, after some time, faults and "profitable repair work";
- though Iraqian weapon computers are "hermetically cut-off from the outside world", computer viruses could be implanted e.g. via "weather data";

 moreover, the built-in computers contain programs which may be triggered remotely; the control system of (French-built) EXOCET rockets could be switched-off from French ships; the only problem would be the mass of weapon computers to be switched-off simultaneously.

As usual in events related to malicious code, truth is mixed up with misunderstandings, errors and impossibilities:

- the implementation of weapon software makes self-reproducing programs (=viruses) impossible; moreover, it is very improbable, that such systems may be (re-)programmed remotely; French "experts" with such arguments are non-trustable;
- on the other hand, other aspects of "malicious code" may well be present in weapon computers; at least in the test phase, rockets can be destroyed by triggering a self-destruction system remotely; following the well-established principle "never change a running program", such "backdoors" (the proper name for this type of malicious code) could survive the test version;
- moreover, French system analysis might well have foreseen scenarios in which to defend against French-made rockets (e.g. EXOCETS); French warships might remotely influence the EXOCET control systems if this remains unchanged by the (Iraqian) users of such technology; with equivalent probability, other Western weapon control systems could contain similar self-protection mechanisms (e.g. US' Hawk missiles having been captured in Kuweit);
- finally, it is well-published (even in non-military periodicals) that and how electronic countermeasures (ECM) may mislead weapon electronics.

Some interesting questions following from such "possibilities":

- May Iraq detect, influence or adapt such weapon software? As software technology is not well-enough developed in Iraq (and most part of the Arab world), they probably must rely on foreign experts (as they evidently do in other Hi-Tech areas).
- If French EXOCET rockets are remotely controllable: why did the French not warn their "friends" who suffered severe losses through their weaponry (e.g., UK in Falkland crisis, or US in the Iran crisis, see accident of USS STARK)? Do they at least now warn and properly equip their allies in the Arabian desert?

For "RISK experienced" experts, it is not surprising that misinformation lives best in threatening situations (such as at the Gulf); apart from general attitudes of newsmedia, computer scientists who nominate their technological constructs (e.g., "self-reproducing programs") in such inadequate terms as "viruses" (see also: "intelligence", etc.) are highly responsible for misinterpretation and misunderstanding by less well informed media people and the public! On the other side, authorities and the public only in such threatening circumstances become aware of riskful assumptions inherent in contemporary computer systems. Such unfortunate experience may lead to the cynical assumption that risks may best be conceived by (hopefully: moderately) "ex post" experiencing them, rather than analysing and avoiding them "ex ante".

Postscriptum: computer "viruses" may nevertheless play a role in "Operation Desert Shield". There are (yet unconfirmed) news items that several thousand PCs (5000?) have been infected by ordinary "computer viruses". This would not be a surprising experience, as the soldiers had to "waste" ample time waiting for Jan.15; in the absence of other possibilities for spending free time, computer games (usually a source of "virus" infections) may have played a major psychological role, maybe with some impact on their "ordinary functional behaviour".

risks of NOT believing war game models

"FIDLER::ESTELL" <estell%fidler.decnet@scfb.nwc.navy.mil> 14 Jan 91 17:34:00 PDT

The risk of NOT believing war gaming models should be revisited, in view of the Congress' vote this past weekend.

In all such "contests" (sports games, wars ...) there is always a chance, regardless of how low the probability, that some rare event may occur; e.g., "mighty Casey may strike out." This is particularly true when one side (or both) have some players with particularly LOW vulnerability, and/or some weapons with particularly HIGH lethality. The outcome of the "game" will vary drastically, depending on what happens to these "superior" players/weapons - and WHEN it happens.

To take a hypothetical case, based on history, SUPPOSE that Gen. Custer had gone into his last stand, with a hundred Gattling Guns; and suppose that those operating these guns had plenty of ammo, and were lucky enough to not be wounded -- at least, until they had done their (dirty) work. One might imagine that it would have been Custer's greatest victory.

IF the Congressional debaters were right, Iraq has some "unusual" weapons; IF these weapons survive long enough to be used, who knows what the outcome might be? The lesson of the Spanish Armada's defeat suggests that Gen. Eisenhower and others were right: After the war starts, no one knows ...

Bob

Re: MoD computer stolen in UK

"Olivier M.J. Crepin-Leblond" <MEEB37@vaxa.cc.imperial.ac.uk> Thu, 17 Jan 91 16:20 BST

Just a quick word to advise RISKS readers that the MOD laptop computer stolen in UK has been recovered by the MOD. The information was in the press last week. There was no mention of any arrest. Understandably, since the gulf hostilities have just started, the MOD is keeping full secrecy about the outcome of the story.

The fact that classified military information was present on the hard disk of a laptop computer would certainly seem to be a risk in itself. It is even more unbelievable that the laptop was left unattended in a car in Acton (West London), which is not the safest of areas in London. I certainly would not leave a laptop (if I had one) in my car in that area !

When computers were as large as a bus, there was no risk of one being "lost" in nature. Now they are so small that one can carry them all around the place. And since a small plastic box looks less important than 20Mb worth of printed paper (with red ink warning notices), it is worrying that the holder of this box becomes that negligent.

Olivier M.J. Crepin-Leblond, Elec.Eng. Dept, Imperial College London, UK.

[The computer's return was also noted by Steve Bellovin (smb@ulysses.att.com), Margaret Fleck <fleck@robots.oxford.ac.uk>, Tim Steele <tjfs@tadtec.uucp> (who added that although the MoD refused to reveal the contents of the note, they said that it convinced them that the data is secure), and Charles Bryant <ch@dce.ie>. THANKS! PGN]

Ke: Computer program gives police a bum rap (Smallberg, <u>RISKS-10.77</u>)

William H. Glass <glass@vixvax.mgi.com> Tue, 15 Jan 1991 00:00:11 CST

In <u>RISKS-10.77</u>, David A Smallberg writes about the problems of a police department determining its crime solving record. This reminds me of a problem I observed years ago while working on a research project studying crime statistics. The city of Philadelphia had one of the lowest auto theft rates of any major city in the US. One of the principal reasons for this was that if the car was recovered within 24 hours (as many are), the crime was reclassified as "joy riding". The Philadelphia police liked this system because it looked like good publicity to have a low auto theft rate. Then, a new federal program was started that among other things gave funding to local police departments based on the number of auto thefts. As you might guess, suddenly Philadelphia suffered a major increase in auto thefts.

William H. Glass, Management Graphics, Inc., 1401 E. 79th Street, Minneapolis,MN 55425Phone: +1 (612) 854-1220Internet: glass@mgi.com

Voting by Phone

Evan Ravitz <eravitz@isis.cs.du.edu> Mon, 14 Jan 91 23:39:46 MST

SECURITY & PRIVACY OF VOTING BY PHONE

The ultimate demonstration that Voting by Phone is reliable is this: we intend to publish not only the election totals, but how each and every Voter ID number voted, so you can check that your vote got through correctly. Since the ID numbers would be assigned anonymously (drawn randomly from a hat, say) nobody could possibly know how you personally voted. Since the "password" part of the number would not be published, nobody could steal your vote at the next election, having seen your ID number in the results. Most usefully, the results could be published on a computer diskette (and be available for inspection at election offices and libraries) so anyone could check that the individual anonymous votes indeed added up to the all-important totals.

This is in keeping with our desire to publish the program that controls the computer that runs the phone election. Currently, all the programs (computers already count most votes in the US) are proprietary software and not open to our inspection and rarely that of the election officials.

The use of "Caller ID" (also called Automatic Number Identification) to identify voters by the phone numbers they call from can be easily defeated by simply voting from any phone other than your own. Eventually special solid-state 'smart cards' used with your phone could encrypt your voting so that you could vote totally anonymously from your own phone as well.

Responding to November's comments:

Voting by phone does not disenfranchise the phoneless! Phone booths are far more common than voting booths and of course the call should be free. Some are always further from the polls than others -- think of rural dwellers, and how this would help them.

In Colorado as well, no ID is needed to vote. They take your signature, but it is not compared to anything unless you are challenged, which would only occur if the judges happened to know you personally. The system is archaic and relies on the judges knowing us by sight.

The problem of the use of caller ID to prevent 'hackers' from constantly calling disenfranchising poor neighborhoods with only 1 phone can be solved thusly: register these phones so the system expects many calls from them. But this is likely unnecessary as most attempts to 'guess' ID numbers will fail -- the system needs to lock out only phones that repeatedly try and fail.

Proxy voting should be criminalized and a reward offered for turning in anyone offering to buy votes. If one expects coercion, 'prevoting' would preempt anyone forcing their choice on you. And since reporting coercion (by phone) would bring a reward this problem would be minimized.

The 'California problem' of voting on so many issues at once is actually another benefit of voting by phone -- why struggle with 40 at once when each could get its own week-long 'slot'? This also makes voting more timely and your ID easier to remember. Phone voting makes this economicly practical.

Telephone service bureaus are prepared now with 1000s of lines for just such applications as phone elections. By opening the lines for several days (voting by mail and absentee are precedents for this) and educating people to spread out their voting, busy signals should be a very small problem indeed.

The main problem of getting the ID numbers to the right people is solved by having them come in to register for the new system, once. This would also prevent them from voting in person as well, just like voting by mail (formerly 'absentee') does.

'Writing in' candidates can be replaced with 'speaking in' their names, along with the spelling. The infrequency of writeins will prevent the transcription from becoming a major expense.

No system is perfect. But phone voting is more secure, inexpensive, convenient, and ecological than our archaic system. That's why most modern business is done by phone-polling, international banking, e-mail, etc. The reason this wasn't done long ago is because it is also the tool for a more direct democracy -- voting on more referenda and initiatives more often -- and this threatens the hegemony of our 'representatives', who now rule with the approval of a diminishing minority of Americans.

The Voting by Phone Foundation can be reached at 774 19th St, #5, Boulder CO 80302 or (303) 444-3596 or eravitz@nyx.cs.du.edu. We'd be happy to send you our brochure, or the E-mail version.

Evan Ravitz, Director

Voting by Phone

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 22 Jan 1991 15:51:51 PST

Evan Ravitz' contribution makes an interesting case, although it fails to adequately address some of our classic vulnerabilities, such as bogus votes inserted by insiders (or outsider/insider collusions). (Insiders could also juggle the expected total number as well.) No one would complain that HIS or HER vote was missing, and yet no one would be able to notice the bogus votes! Another problem is that people would tend to write down their ID/password, and either forget it or lose it between elections. Insiders could also wait until the last minute before closing time and instantaneously vote for those who hadn't yet gotten around to it. But there is much merit to the idea. PGN

Word processor atrocities

Pete Mellor <pm@cs.city.ac.uk> Mon, 14 Jan 91 09:49:20 PST

On the general theme that a word processor does for words what a food processor does for food, in his column in the Observer on the Sunday before last, Simon Hoggart recounted the tale of a novelist who decided at the last minute to change her main character's name from David to Jeff, with the result that a piece of dialogue about sculpture referred to the previously unknown work "Michaelangelo's Jeff".

He followed it up last Sunday with a medical study which was originally written with the family name of the subject of the research given only as "B", to preserve confidentiality. For some reason, it was decided that the full name could, after all, be used, which led to the discovery of the new disease



Peter G. Neumann <neumann@csl.sri.com> Wed, 23 Jan 91 15:00:23 PST

Excerpted [by PGN] from today's Wall Street Journal (23 Jan 91) and AP items.

[Lotus Development Corp. was expected to announce today that it will drop its plans to place on the marketplace Lotus Marketplace, discussed here copiously in earlier issues (RISKS-10.61,62,63,68,74).]

"The turnaround on Marketplace suggests that technology companies are slowly learning how to strike a publicly acceptable balance between privacy and the explosion of electronic data. One example came last year when phone companies introduced "Caller ID" options that flash a caller's number on the other party's phone. In response to consumer complaints, some phone companies are adding a feature that lets callers block their numbers." [WSJ]

"Lotus said it also would discontinue shipment of Lotus MarketPlace: Business, a database of information on 7 million U.S. businesses. That product had been offered since October." [AP] [The WSJ article implied that this product would NOT be cancelled.]

``Marketplace touched a raw nerve among consumers, and took on a broad symbolic

significance in the debate over electronic privacy. When Lotus offered to delete data about anyone who called or wrote, it was flooded with about 30,000 requests. Consumers learned about the product through widespread news reports. ... Marketplace also became one of the hottest topics on the computer networks linking technology students and professionals. Complaints and protest letters were posted an copied on hundreds of networks. Opponents circulated Lotus's phone number and the electronic-mail address of Jim Manzi, its chief executive officer. "If you market this product, it is my sincere hope that you are sued by every person for whom your data is false, withe the eventual result that your company goes bankrupt," declared one letter to Lotus that was posted on several networks." [WSJ]

"Privacy advocates' chief objection to Marketplace was that it wouldn't be easy enough for consumers to delete their data, or correct any inaccuracies. They worried that even if Lotus offered to update the disk with corrections and deletions, offending earlier versions would still go on sale." [WSJ]

``Lotus and Atlanta-based Equifax spent two years developing Marketplace Household. Lotus spokesman Richard Eckel declined to estimate Lotus' development costs.'' [AP]

""There was no effective way to make sure that everyone listed on that product had freely consented," says Marc Rotenberg, Washington director of Computer Professionals for Social Responsibility. The nonprofit group was one of Marketplace's loudest opponents." [WSJ]

And then there was this item, contributed roundabout, in a memo today from Jim Manzi to Lotus and Equifax folks, announcing the demise of both products:

"Unfortunately, we feel the majority of concern over the Households product has been generated by misinformation about the product's content and a general lack of understanding about the direct marketing industry. From the very beginning, Lotus and its data partner, Equifax Marketing Decision Systems, implemented a number of privacy-related controls that exceeded traditional direct marketing industry practices. We felt confident that these procedures limited any potential abuse of the product. Consumers should demand that future products of this type be as scrupulous and responsible." [Jim Manzi]

[The WSJ item was noted by Sean Kirkpatrick <sean@NISD.CAM.UNISYS.COM> and others. The AP item was noted by Steve Bellovin <smb@ulysses.att.com>; an earlier personal phone call to Lotus attempting to get himself removed from the database resulted in Scott Wilson <swilson@pprg.unm.edu> being told that there would be no database from which he could be removed.

On Monday, Roger H. Goun <goun@ddif.enet.dec.com> noted an article in the Boston Globe Business section, T.G.I.M. column, 21 January 1991, the writer of which included the following premonition to those who wanted to object to their being in the database:

Save your breath, and save Lotus the dime. They're getting the message. If I were a betting man, I'd bet you won't see Lotus in this Marketplace much longer. And yes, for you skeptics, there are still 10-cent payphone calls in Massachussetts, among other places, although the incoming 800 number is probably not exactly 10 cents per call. PGN]

🗡 UK firms poor on computer health

"Olivier M.J. Crepin-Leblond" <MEEB37@vaxa.cc.imperial.ac.uk> Thu, 17 Jan 91 16:19 BST

This article has appeared in a specialised publication in UK called Technology Graduate, Nov/Dec 1990 issue.

British companies are not doing enough to safeguard their employees against the health hazards of working with computer technology. Only a quarter of businesses take formal health and safety measures, according to a survey published in "Which Computer ?" magazine.

A sixth of the organisations who took part in the survey reported staff illness directly related to the use of information technology equipment, injuries such as headaches, repetition strain injuries (RSI), eye problems and back, neck, wrist and finger ailments. A third of them said they received staff complaints about the health risks associated with computers.

However, employers will soon be compelled to take statutory action on the welfare of staff. By the end of 1992, EC member states have to put up with a directive which lays down minimum health and safety requirements for work with IT. Employers will become legally responsible for ensuring that all new equipment installed meets its requirements; existing equipment must be brought up to standard within four years.

The directive also governs mandatory inspections of computer equipment and sets down minimum standards for the ergonomic design of computer screens and keyboards, desks, seating and lighting.

It provides for training and organisation of time to allow for periodic breaks from screen work and regular free eye tests and glasses where necessary.

Display screens must be flicker-free and fully adjustable. The keyboard must also be separate from the screen. Sufficient desk space must be provided for hand and arm support. Computer users' chairs must be adjustable and a footrest must be available on request.

Many of the companies surveyed were ignorant of both the risks and of where so seek advice on computer health and safety. Less than a quarter had consulted the Government's Health and Safety Executive on computer users' rights and only one in 10 had taken advice from an ergonomist. "

- Typing this has given me a backache. -

Olivier M.J. Crepin-Leblond, Elec. Eng. Dept, Imperial College London, UK.

[Cogito, ergo nomics.]

Data privacy abuse in Australia

Phil Clark <pgc@csadfa.cs.adfa.OZ.AU>

17 Jan 91 00:44:26 GMT

The following items appeared in the "Canberra Times" of Monday 14th January 1991 and Tuesday 15th July 1991. These show how computer information, databases, banking and credit records are being abused in Australia, with little or no recourse for the general public.

IN 1990 THE Commonwealth Privacy Commissioner published a thick report listing the extensive tabs the Government keeps on its citizens, including details on people's sexual lifestyles and relationships, held by the Department of Immigration, local Government and Ethnic Affairs.

It showed that dossiers are created on people who write to government ministers, and that the Federal Government has access to all state birth, death and marriage registers and state vehicle and licence authorities' records, which it matches up with Medicare, taxation and social-security files. The Taxation Office collects information on Medicare records, bank accounts, land-title records, car registration and virtually every immigration movement into and out of Australia, and the Department of Employment, Education and Training has access to most university records.

The flow of personal data in Australia is generally freely swapped between state and federal governments. In 1990 the Government passed the Cash Reporting Transactions Act, which effectively makes the banking industry an arm of government, providing details on major transactions, and which is rapidly moving towards the Government having full on-line computer access to people's bank accounts. Even the NRMA (*NSW motoring organisation) gives its three-million-name membership list to help the authorities track down unpaid parking fines.

Australia lags far behind France, Germany, Singapore, Belgium and Austria, which have detailed laws protecting privacy. This prompted, by the mid-80s, a series of European media reports detailing Australia's departure from the norms of developed countries. Among examples are NSW laws allowing people to be taken into custody without being charged and forced to give blood, and, more recently, laws dealing with the search and seizure of private property.

One of the most far-reaching of recent laws is the one that confiscates assets 'SUSPECTED' of being the proceeds of crime or even associated with crime. It can deny the accused access to his money for legal representation, and in some cases reverse the onus of proof.

Some of these state laws directly depend upon the ever-increasing information flow to round up suspects. Many people so accused have been innocent, chosen for investigation simply because they fitted a certain computer profile, such as a businessman arrested because he travels overseas a lot and appears to the computer as if he might be a drug courier.

In a recent radio interview presented by the wife of the NSW Premier, Kathryn Greiner, it was revealed that a woman had wrongly been reported to the Taxation Office as running a brothel. The information was reported to the Government by her credit union, to which she had applied for a loan.

The Cash Transactions Reporting Act in the past six months has caused dozens of innocent individuals' lives to be invaded by the authorities. In some cases their homes have been seized. Most Western European countries strictly prohibit the collection and networking of data. The next step is the introduction of a Bill in a few months requiring Australian citizens to have an exit visa before being allowed to leave the country.

Partly in response to the criticism of the European Press and growing concern of Australians about privacy, the Commonwealth Government enacted the Privacy Act. The preamble specifically recites Australian obligations to protect personal privacy under the International Covenant on Civil and Political Rights.

The main Act relating to Commonwealth records was passed in 1988, with an accompanying Bill which purported to regulate the activities of credit-rating bureaus. After heavy lobbying by the finance industry and the Credit Reference Bureau of Australia Ltd, the Bill was delayed.

The Act gains nation-wide coverage by a backdoor method to overcome constitutional limitations. The thinking of the Government in drafting the legislation relies upon reform of the way organisations collect and manage information. The linchpin is the commissioner's power to create a Code of Conduct which if breached gives the commissioner the power to award compensation - a duty he has been given to enforce with just 11c per Australian. As the general manager of the Credit Reference of Association of Australia Ltd points out, at the time of drafting the prosecution provisions were rarely (if ever) expected to be used.

The reality is that the privacy legislation already a complex 90-page hotchpotch of provisions unable to be read without reference to other legislation, offers little real protection of privacy and even less compliance with the spirit of the treaty to which it supposedly gives effect.

The Privacy Act is being used by the Government to add a further obstacle on top of the already restricted Freedom of Information Act to deny information legitimately sought by journalists. An example is where ministers' officers refuse to comment on cases by saying erroneously that the Act prohibits them from saying anything.

It exempts intelligence agencies, the National Crime Authority, most activities of government enterprises, and Royal commissions and government ministers. The information can be used for any purpose or exchanged "for any other purpose" where the Government believes a person impliedly agreed to such a release.

Because most government-agency forms contain broad boilerplate clauses which provide for the exchange of information, implied consent "for other purposes" will nearly always be present. For example, the Department of Immigration, Local Government and Ethnic Affairs places on its forms that it is the department's "usual practice [to] pass on some or all such information to agencies which deal with education, health community services, social welfare, employment and labour, intelligence, law enforcement, taxation and statistics".

As it stands, the legislation is sufficiently vague to offer Commonwealth agencies wide discretion in deciding what constitutes implied consent and what

is meant by the word "reasonable". Similarly, the legislation provides a blanket clause that allows private information to be given out where it is "reasonably" necessary for the "enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue". It allows Social Security to match up its records against tax and income details held by other departments, a practice recently entrenched by data-swapping legislation passed in the last week of parliamentary sittings.

The exchange of information currently extends to Social Security getting lists of drivers from taxi companies so it can look for pensioners and the unemployed attempting to earn a few undeclared dollars. Its computer combs state death registers to identify deceased beneficiaries. Unfortunately the same procedure has led to embarrassing errors where innocent people have had their income stopped because of a mistaken identity.

Social Security and Taxation also use the Credit Reference Association of Australia Ltd to investigate people's finances.

The legislation is wide enough to cover also the release of information for ANTICIPATED evasion of any law, such as state stamp duties, investigations or, for that matter, nearly any act of a state government which has a connection or responsibility of administering a government Act. In other words, the exceptions are so wide as to empty the legislation of any real clout.

The legislation fails to address a general fear of the spectre of a 1984 "big brother" that is an all-knowing omnipresent surveillance, because it does nothing to control effectively the real mischief which lies in cross-linking the records which affect a person's life.

Except for tax-file-number information, few controls are put on what state governments do with information given to them by the Commonwealth. With up to a dozen government agencies swapping data, a large number of people learn secrets, and information may become less accurate on each transfer.

In recent times there have been a number of prosecutions against Social Security staff, tax officers and other public servants selling data-base information, police in various states accused of selling motor-traffic and other government information, and other illegal passages of information. Private investigators have boasted of how easy it is to extract information. The average person has reason to have serious doubts as to privacy within state government records with which the Commonwealth freely swaps data.

The Privacy Commissioner, former barrister Kevin O'Connor, appointed to administer the Act operates under a number of fetters, including a curious provision requiring him to have regard to "social interests that compete with privacy including the general desirability of a free flow of information and the recognition of the Government and business to achieve their objectives in an efficient way". This is wide enough to force the commissioner to take into account government policy aimed at matching up its records and creating detailed profiles of people's spending patterns for taxation or any other type of investigations the Government thinks desirable.

At present the commissioner works on a tiny budget of just over \$2 million a

year, which is grossly inadequate to carry out his enormous task. He is also muzzled by extraordinary provisions which' enable the Attorney-General to certify that he may not investigate certain breaches of the Act by the Government for such ill-defined reasons as national security, international relations or where an investigation is planned or where the matter concerns the methods and practices adopted by law-enforcement or intelligence-type agencies, despite that it is in this very area that the greatest fears for personal privacy exist.

The commissioner has limited powers to award compensation in certain cases although the legislation is silent as to how much and when this provision may operate. How can a person put a value on having put on public display his personal affairs, which will never be the same again? How to value the feeling of being personally invaded and the hassle of clearing it up? To give the legislation some teeth, the commissioner will need to take a robust attitude in order to make organisations responsive and to encourage aggrieved individuals to take the time and trouble to make and follow through a complaint.

Yet even where compensation is awarded, if the person against whom the order is made refuses to pay, then the whole matter is reheard by the Federal Court, an expensive and time-consuming process where legal costs can quickly wipe out any compensation payment.

Tomorrow: Credit reporting agencies.

The Credit Reference Association of Australia is the largest credit-reporting bureau in Australia and is jointly owned by the banks, insurance companies and to a lesser extent its smaller subscribers. It has records on about nine million adult Australians.

Amendments to the Privacy Act that claim to control this agency were passed in the last fortnight of the 1990 Parliament and heralded by Senator Nick Bolkus (Lab, SA) as one of the great reforms of the Labor Party. The Bill was originally introduced in 1988 but stalled for two years while heavy lobbying took place behind the scenes.

According to the general manager of the association, Bruce Bagon, it hired former Commonwealth Ombudsman Jack Richardson to draft model legislation for its own governance.

Contrary to the great achievement claimed by the Government, the recent amendments to the Commonwealth Privacy Act were not new because the association had already been restricted since the 1970s under various state legislations and by its own internal policies.

The effect of the new legislation, which does not become law for another nine months, claims to restrict who can gain access to consumer files by allowing access to only "credit providers". This means that many peripheral users such as real- estate agents, Telecom and insurance companies can no longer get credit information.

It also prevents "positive reporting" being placed on a file - something the association had at one stage planned to introduce. Positive reporting puts a person's current details on file, whether positive or adverse, such as current

credit accounts held and balances owing on each account, payment details and so on.

Other provisions force the association to separate - but not delete - a person's "commercial" activities, such as whether a person is a director or otherwise associated with a failed company or a business.

It also requires publicly available records such as electoral-roll information and telephone-book information to be stored separately, but not deleted. The law still allows court judgments and bankruptcy notices to be included on a person's file.

Similarly, insurance records will be separated.

The result will be that most people will have three files, one for personal credit, another for insurance, with a last one holding information on any "commercial" activities.

As with the provisions of the Privacy Act that claim to regulate government files, the parts that regulate the credit bureaus contain numerous loopholes. The association's general manager says the legislation adds very little to its existing practices, except to cause the separation of files. It creates a vague list of "privacy principles" and requires a "code of conduct" yet to be formulated to cover the nitty-gritty details of regulation, such as how to decide what constitutes a person's "commercial", as opposed to personal, financial activities.

The federal legislation does not give consumers a specific right to directly ask the credit bureau to remove errors, in contrast to legislation in countries such as the United States, which has had a Fair Credit Reporting Act since 1971.

This weakness forces customers to go through their credit providers to have the error completely removed. As the credit provider has no financial incentive to correct records actively, it in effect puts consumers in the position that the banks decide when and what to tell the credit bureau. There is virtually no chance of successful prosecution.

The only restriction placed on the credit provider is that it must tell the bureau "as soon as practicable" that a person has paid an outstanding bill or denies liability. In practice this allows the banks the flexibility to delay making corrections while it "investigates" any other type of error. The consumer's only direct right is to have a note added to his file stating that there is an error.

But, unfortunately for the consumer, the maxim "no news is good news" is especially relevant in the credit industry. Despite any note on the file, a consumer is unlikely to be given the benefit of the doubt by another potential credit provider.

The result is that the consumer is effectively at the mercy of the banks as to when they decide to act on a complaint - a disheartening prospect considering the poor service that seems prevalent with banking nowadays. The US legislation, by contrast, foresaw this problem and requires any disputed negative items to be removed until (and if) the matter is cleared up. The bank that made the negative report has 30 days to justify its claim, after which the negative item permanently lapses.

Although the legislation claims to restrict the use of information for the purposes of assessing credit applications, it can be used for many other purposes if it believes on "reasonable grounds" that a consumer is no longer willing to comply with his obligations.

Then the legislation allows the information to be used "in connection" with the consumer's alleged lack of compliance. This gives great latitude to credit providers.

In modern credit-management practices, if a person refuses to return phone calls, refuses to do as the creditor asks or perhaps refuses to discuss the matter, the consumer runs the risk of being labelled as "delinquent" or as a "skip", with the result that other credit providers are given the names on a special alert list.

Just what "reasonable grounds" means to a credit provider or in-house debt collector is unspecified, unlike the US law, which sets up a specific regime.

There is little chance of successfully prosecuting credit providers or reporting bureaus. A prosecution must prove corporate criminal liability - difficult to establish at the best of times but almost impossible under the new legislation.

The Privacy Act requires that the entity must knowingly or recklessly breach the Act; show that the employee who committed the act in question did so within the scope of his actual or apparent authority; have the requisite state of mind; and finally requires proof that it failed to take reasonable precautions and to exercise due diligence. Each of the four criteria must be proved beyond reasonable doubt. Privacy legislation in Australia therefore offers very little to the public.

The various principles and unstated practice codes are so widely defined as to be meaningless and/or easily interpreted in such a way that nearly any act can be justified with-in its framework.

With the likelihood of successful prosecution virtually nil, the legislation does protect tax-file numbers but, far from the breakthrough claimed by the Government, it remains little more than window dressing.

The Government needs to bite the bullet and use its external-affairs power to create a uniform and detailed law on privacy for the whole of Australia, written m plain English in a consolidated Act.

Phil Clark [VK1PC] Department of Computer Science, Australian Defence Force Academy, Northcott Drive, Campbell, Canberra, Australia, 2600. +61 6 268 8157

MasterCard policy opens door to crooks.

&arv_Westrom@mtsg.ubc.ca> Mon, 21 Jan 91 09:56:48 PST

I have a MasterCard account which I use regularly. I keep my receipts and match them to the line items on the statement each month. On January 15th I received a regular statement which contained an item for which I did not have a receipt. A phone number is provided on the statement; I telephoned Customer Inquiry to ask further about the charge. Possibly I had lost the receipt; or possibly the charge was made incorrectly.

A man identifying himself as Warren informed me that they could not provide me with a copy of the sales receipt, and the only way to address this matter was for me to write a letter (to Julia) explaining that the charge was incorrect. There was a second charge to the same merchant (an EXXON station) on the same day and upon learning that I still had my copy of this sales slip, he explained that a photocopy of it would be required with my letter so that they would have proof of an erroneous charge. I felt that these demands defied common business practice and all common sense but he assured me that this was company policy.

MasterCard is a significant presence in our society. I use both MasterCard and Visa as a part of my regular personal financial activities. These two companies have a virtual monopoly on this form of credit; I do not have the opportunity to take my business elsewhere. So perhaps they can use their monopoly power to institute a policy that is contrary to common sense. But I don't think they should be allowed to do so.

An unscrupulous person knowing that this was MasterCard policy could set up a system of generating unwarranted charges with some cover of plausible deniability. Many of these charges would be paid simply because customers do not check their accounts closely. But even those who notice the spurious charges now have the onus of taking action and proving that they did not incur the charge. For a charge of \$30 or so, many people would pay up rather than get involved in the hassle of proving that they did not owe it.

What protection do I have from spurious and unwarranted charges to my MasterCard account, from unscrupulous merchants who could note my number and then put through fictitious charges and from errors by cooperating merchants and MasterCard itself? I can see that MasterCard would wish to be relieved of the burden of being honest and accurate, but surely the onus for proving that I owe money has to be on them. Notwithstanding that this is contrary to company policy.

I will write my letter to Julia and enclose the proof that she requires. But I think that MasterCard's policy in this matter is a significant and serious deviation from acceptable practice and poses a significant risk to us all.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



* 7th Chaos Computer Congress, Hamburg, 27-29 Dec 1990

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 24 Jan 91 14:19 GMT+0100

In its 7th year, the annual conference of Chaos Computer Club was held in Hamburg (Germany) in the last week of December. A broad spectrum of themes was offered, dominated by networking, but also covering legal aspects, ecological computing, freedom of information, female computer handling, psychology of hackers and others. Among the more than 300 participants, only few people from European countries (Netherland, Italy) and USA participated. The Congress newspaper (covering reports about most sessions, available as *.DOC or *.TXT files, see below) is only in German. Though the printed (DTP-ed) version of it looks more professionally, some essential discussions (e.g. female computer handling, computer viruses, the new German Information Security Agancy, GISA) are missing; quality and readibility of articles is rather mixed. As there were only few spectacular themes (phreaking, copying bank cards), public interest and coverage in newsmedia, as compared to CCC'89 (the year, when the KGB hack was published) was moderate. Among the spectacular themes, a group HACK-TIC from Netherland demonstrated a machine (about 1,500\$) to copy credit and Eurocheque cards (EC); according to Wau Holland (co-founder of CCC), this was arranged "to demonstrate the insecurity of these plastique cards". While the speaker of Hamburg's saving bank (HASPA, which was the victim of CCC's famous "Btx/HASPA-attack") said that this is impossible, a journalist of BILD (a German boulevard newspaper) received a printout of his account with a copy of his card, but when trying to order money from a teller machine, his card was collected.

The most spectacular event was a workshop on (phone) "Phreaking". Experiences and methods how "to call as far as possible with as many phreaks as possible at lowest possible price" were described in some detail (few of which were written). Tricks with German PTT's 130-number (and connection to US' 700/800 numbers) as well as with the (PTT-internal) test number 1177 to establish low-cost (at least for the phreaks) teleconferences and voice mailboxes were discussed. It is surprising to hear from a US phreak that the old tricks (2,600 MHz, red boxes to simulate the coins' click) even work today; some new experiences esp. tricks with Calling Cards (due to missing expiration date on some cards or delayed update of MCI databank) were added to "help fight the excessive telephone costs". Dutch phreaks informed about "use" of 008-numbers; a hotel reservation service at a large airport doesnot check the validity of credit cards (file: PHREAK.DOC). The workshop was not concerned with legal aspects of Phreaking.

Several sessions were devoted to networking. Chaos Computer Club runs a network ("Zerberus") with gateways to international networks and a growing number of regional mailbox systems. Despite mixed (or even bad) experiences with new mailbox systems and gateways (the gateway group emailed invitation to this workshop; 50% of the invitations came back, essentially with "error-mail"; file NETWCHAOS.DOC), several sessions were devoted to introductions into networking (file WSI-NET.DOC covering a detailed INTERNET survey; several files on GATOR, a GATEway ORientation guide to regional and international communication and gateways). A special report was devoted to communication of graphic and sound data, where special standards, command languages and software are under development (file SCF.DOC). Special discussions were devoted to applications of mailboxes for ecological purposes (file UMWE-DFU.DOC) and as infrastructure for publications (file Med-DFU.DOC), as well as to aspects of (German) publication laws (file PRESRECH.DOC).

One session was devoted to CCCs idea to aid the former GDR (now "5 new federal countries") in establishing a citizen computer network "DDRNET". Despite of significant aid by computer dealers (who spontaneously donated PCs, software and modems in significant numbers) and despite of the interest of local groups and parties (New Forum, essential force in the East-German revolution), tax and organisation problems finally stopped the project when German reunification happened. The document (file: DDRNET.DOC) gives a lively example of good ideas and plans being killed by hostile bureaucracy.

Following earlier CCC' discussions on sociological aspects of hacking, a student (Tommy) described his examination thesis (diplom work) relating Psychology and Computing (file PSYCHO.DOC, thesis in compacted form: PSYCH.LZH in 109kBytes). According to Tommy, hackers exhibit their self-consciousness as an elite by their techno-speak. "Ordinary" people of same age with no

understanding of computing are rather suspicious about hackers, even more as computers appear as threats to their civil rithts and working places. In such controversies, hackers seems to flee reality, mostly unconsciously, and they live in simulated worlds such as Cyberspace ("not as dangerous as other drugs"). Anonymous or technically depersonalized communication (e.g. mailboxes) lowers the threshold of moral scruples, resulting in communication garbage and flames. Btw: as in previous years, a special workshop on Cyberspace demonstrated EEG-coupled graphical devices and software (file: CYBER.DOC); the sub-culture (as initiated by Gibson's book "Neuromancer") developing around this techno-drug has it's first European magazines (Decoder, Cyberpunk).

A special discussion developed on computer "viruses". Two speakers working with Ralph Burger (author of the "Big Book of Computer Viruses", also publishing virus code in German, English and Russian) described his work to classify new viruses and to establish a databank of virus code. In their classification, the group starts with a specific model of virus mechanisms including self-encryption; this model is in some contradiction with other classification (e.g. as a virus in their model must always have an effect, parent viruses like DONOTHING having no effect would not be a virus while their descendants are), and stealth mechanisms other than encryption are not foreseen. The speakers argued that information on virus details should be easily accessible to all relevant parties.

A controversial discussion arose when the author of this report informed about the establishment of CARO (=Computer Antivirus Research Organisation, cofounded by V.Bonchev/Sofia, Ch.Fischer/Karlsruhe, F.Skulason/Rejkjavik, A.Solomon/UK, M.Swimmer/Hamburg, M.Weiner/Vienna and the author) to establish a database with virus specimen and procedures to quickly analyse new viruses and distribute the disassemblies for verification and antivirus developmernt. As the number of viruses grows significantly (more than 400 MsDos viruses known, plus new developments visible in Soviet Union, Hungary etc) with advanced stealth methods and more sophisticated damage, restrictions in the access to such virus specimen based on concepts of "trusted persons" and "need to know" are presently discussed (also controversially). In contrast to such concepts, CCC'90 participants and the speakers expressed their view that such virus specimen should be accessible to any interested party.

Summary: apart from the session on phone phreaking, Chaos Computer Club visibly demonstrated its distance to criminal activities which dominated the last conferences (e.g. KGB hack). In discussing themes of technical and related interests, they return to the list of items which were described in their foundation document (file THESEN.TXT, October 1981). Themes related to civil rights (e.g. "Freedom of Information") are visibly of more interest than classical hacking techniques. As CCC didnot discuss any consequences of the KGB case (after the trial in March 1990) for its members or related persons, CCC omitted the opportunity to prepare for it's role in future hacks in it's environment. While their annual conference was less chaotically organised than last year, it's structure and future developments remain as the name indicates: chaotic and computer-minded, yet with a sense for new ideas and applications.

✓ San Francisco taxes its computer people rather than its property owners

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 24 Jan 1991 12:02:03 PST

Last year, as many as 8700 San Francisco property owners did not receive their annual tax bill (normally arriving by 1 November). A "computer glitch" in the tax collector's office was blamed for not sending bills to owners in the "default" category (as a result of having missed or been late on a previous payment).

[Source: San Francisco Chronicle, 14 Dec 1990. I finally got around to entering this item, even though it is now old-hat. However, I haven't seen anything further about the problem being fixed, although it presumably has by now. Surprisingly, the Tax Collector was quoted as saying he did not think they would lose money because of the delay! Not much interest in getting it fixed? I would think there would be interest LOST from NOT getting it fixed.]

Not risk versus convenience, but risks of conveniences

Jack Campin <jack@cs.glasgow.ac.uk> Wed, 23 Jan 91 20:28:58 GMT

>From the Glasgow Herald, 18 January 1991:

Superloos reveal all	by Graeme Smith
*****	********

Vandals who tangle with a new (pounds) 50,000 superloo in Aberdeen face the prospect of having their misdemeanours revealed to all.

Apparently the most advanced convenience in the world allows undesirables just 1.7 seconds of misbehaviour before it throws open its door to reveal their misdemeanours and sprays them with violet coloured dye which will remain on their skin for at least five weeks.

If, however, you are there for legitimate purposes it will allow you 15 minutes of luxury for just 10p. The air is perfumed, as well as heated, there is background music to help you relax and there are special facilities for the disabled and for baby changing.

When you have completed your business and safely departed the superloo spruces itself up for the next customer. The walls, floor and WC automatically wash themselves down and when the disinfecting cycle is completed the WC is dried with warm air.

It is careful to ensure that thrifty Aberdonians do not try to sneak in two at a time to half the cost, or for any other purpose. It will happily allow a mother with children and a pram to enter but if two adults step inside, the computerised equipment which the importers claim is sensitive enough to tell the size of your shoes, will prevent the door closing.

Three have been commissioned in Aberdeen this week, one in Byron Square in Northfield, one in a layby on the Stonehaven road on the outskirts of the

city, and the third at North Deeside Road.

(Any Aberdeen readers brave enough to try changing their shoes in one? - jack)

Jack Campin, Computing Science Department, Glasgow University

Ke: Computer program gives police a bum rap (<u>RISKS-10.77</u>)

Mark Hull-Richter <mhr@ccicpg.UUCP> Wed, 23 Jan 91 11:22:09 PST

It is with great interest that I read the referenced article. Of all the police departments in the state of California, I would have thought that the Long Beach Police were the least capable of being given a "bum rap", least of all by a computer program.

Unless things have changed drastically in the last few years, the Long Beach Police Department is the most likely to deserve a "bum rap". They had a policy (unofficial, of course) many years ago of not investigating crimes which they considered to be unimportant, even when they knew who the perpetrator(s) were and that there was evidence of same. Perhaps this was limited to the low-rent areas with high Hispanic concentrations in the population or other poor areas of the city, but this happened over and over again during the late 70s and early 80s (last I checked).

Furthermore, the Long beach Police Department is the one wherein seven police officers were sued for the wrongful death of a man who was murdered by LBPD officers in a case of mistaken identity. This was fairly well-documented in the press at the time. Summary: four police cars with seven police officers were called to a house late in the evening to apprehend a suspect in a series of crimes. The suspect was taken out to the police cars where he was beaten to death by the police despite the fact that, according to witnesses, he did not resist the arrest in any way nor was he armed. It turns out the man was the _wrong_ person, selected (I think) incorrectly from a partial license plate and his slight resemblance to the real suspect.

Brutality and refusals to enforce of the above nature used to be common in Long Beach. I don't know if they still are, but I would be greatly surprised if not. Thus, I find it difficult to believe that the computer programs actually gave them a bum rap. In fact, it wouldn't surprise me if the LBPD actually abandoned cases they couldn't solve within one month, hence the reporting.

Mark A. Hull-Richter, ICL North America, 9801 Muirlands Blvd Irvine, CA 92713 (714)458-7282x4539 UUCP: ccicpg!mhr

M Re: Lotus Marketplace

Richard A. Schumacher <schumach@magnum.convex.com> Thu, 24 Jan 91 19:56:58 -0600

So Lotus will withdraw its product, and everyone will go home happy and

satisfied that they have preserved their privacy. Well, as faculty at the University of Wisconsin - Madison and elsewhere have told me informally, these people are wrong. Everything that Lotus was offering on CD-ROM is already available at "substantially" the same price and conditions; these academics say they are puzzled about the uproar, since in their opinion Lotus offered nothing new.

If we want to truly change things it will take new laws and new attitudes in the business community concerning what information it is acceptable to gather and use. Halting this one form of marketing won't change anything by itself, but it can be the opening skirmish in the necessary public relations war.

MasterCard policy opens door to crooks (Re: Westrom, <u>RISKS-10.79</u>)

Steve Pozgaj <steve@dmntor.uucp> Thu, 24 Jan 1991 09:54:46 -0500

> A man identifying himself as Warren informed me that they could not provide me
 > with a copy of the sales receipt, and the only way to address this matter was
 > for me to write a letter (to Julia) explaining that the charge was incorrect.

This sounds bizarre. In the 20 years I've been a MasterCard holder, I've had this problem twice. Each time I was told that they would indeed send me a copy of the slip [shich they are legally bound to keep for some number of years]. However, if it turned out to be mine legitimately, then I would be charged a ~\$6 processing fee. If it was indeed not mine, no charge would be incurred. (In both cases, it was not my charge!)

So, I believe your "Warren" is simply misinformed, or the laws protecting consumers in the US are seriously worse than those here in Canada. However, there still remains an irk: I got no reimbursement for the money that they had forced me to pay while the credit was being processed. This I find rather despicable. I was told by my "Warren" that if I didn't pay the amount as due, I would be charged interest on it, and, EVEN IF it were not mine, hell would freeze over before I got the interest credit.

So, even though the charge was erased, I was out of pocket, without compensation, for the approximately 8 weeks this all took. On ~\$200 at the then-current rate of 10% savings account interest, that represents about \$3!

Steve Pozgaj @ Digital Media (steve@dmntor)

"Mastercard" Policy

<[anonymous]> Wed, 23 Jan 1991 18:47:31 PST

It is worth nothing that almost all issues relating to charges, errors, credits, etc. on VISA and MASTERCARD statements are under the control of the particular bank/financial institution issuing the particular card and/or merchant account in question. VISA and MASTERCARD themselves are primarily

umbrella organizations for properly allocating purchase charges and credits among the member financial institutions. While VISA and MASTERCARD do have umbrella security regulations, the sorts of problems mentioned by a recent writer to RISKS should be addressed to the financial institution directly. Since policies on such matters vary widely between institutions, blaming VISA or MASTERCARD themselves is probably a misdirected effort.



Search RISKS using swish-e

Report problems with the web pages to the maintainer


Sanford Sherizen <0003965782@mcimail.com> Fri, 25 Jan 91 21:06 GMT

A recent review of a book on developments in forensics mentioned that the use of dental records to reconstruct the identities of bodies was not as successful as once thought. The technological developments for the reconstructing of identities has advanced but the limits are from the original dental records. Some dentists have not been recording the true dental history of patients but have structured their records to reflect the categories that insurance and other third party coverage plans use for repayment. This is also a problem with physicians, who have been treating patients for one problem but reporting patient treatments with an eye toward what payment structures allow.

This does not have to mean that proper assistance is withheld. It just points to the social limits to relying upon technology.

Sandy Sanford Sherizen, Data Security Systems, Inc., 5 Keane Terrace, Natick, MA 01760 (508) 655-9888

Kinking Foreign-sold Military Equipment

Karl Lehenbauer <karl@sugar.hackercorp.com> 26 Jan 91 03:16:47 CST (Sat)

As the complexity of software in military equipment increases, it will be ever easier for a contractor to slip a kink in. For example, a special message, cleverly sent, turns off a jet's engines, changes a missile's course, etc.

As today's allies can quickly become tomorrow's enemies, and hardware a country exports can end up being used against it, there is some incentive to code in an "insurance policy."

This would be a two-edged sword because an enemy of your client-customer could discover a kink in something you sold them, and use it against them.

I have often wondered whether the Star Wars people plan to include a way to turn off the several thousand "Brilliant Pebble" space-based anti- ballistic missiles, if they were ever to be deployed. Being able to update the software remotely would be desirable too, to put it mildly. It would seem an essential requirement, yet it is easy to imagine our guys building and launching thousands of these things without an off switch for fear that the Soviets would figure out how to turn them off or reprogram them, and some terrible possible consequences (of not having a way to switch them off), like bugs causing the pebbles to attack satellites and spacecraft. uunet!sugar!karl

Patriot missiles

Phil Agre <phila@cogs.sussex.ac.uk> Sat, 26 Jan 91 18:22:50 GMT

The Patriot missiles genuinely seem to be working well, at least in the desert environment. Yet a few years ago the Patriot was the very prototype of the incompetent high-tech military development program. Its testing in particular came in for congressional ridicule. What happened? According to its manufacturer and to various other experts quoted in the press, its software was greatly improved through the application of software technology developed for SDI. These experts regard the success of the Patriot as evidence that the SDI's software nay-sayers were wrong. I am willing to calm down for a minute and give this proposition a serious hearing. Has anybody got any details?

Phil Agre, University of Sussex

✓ Electronic cash completely replacing cash

"David 'Witt' DTN 226-6044" <wittenberg@ultra.enet.dec.com> Fri, 25 Jan 91 12:16:14 PST

I'm sure I don't have to go into all the RISKS of this, but it is very scary. The comments at the end that are meant to be reassuring are the scariest part. He seems to be completely oblivious to people's desire to keep some information private, even from the govenment.

The problems of reliability are also obvious.

--David Wittenberg

[I didn't see the original article, so I only trust that this is transcribed accurately. --dkw]

The New York Times, Saturday, December 29, 1990

Three Radical Proposals that could transform New York City, the nation and maybe, the world. by Harvey F. Wachsman

Abolish Cash (Great Neck, N.Y.)

With the nation's economic tailspin causing the loss of tax revenues, the President and the Congress are going to be considering a variety of options that no one will like: raising taxes, cutting services or both. But before they increase the burden on the American people, they should consider a system that would collect all the taxes that are already owed.

If all the people who do business in cash were forced to report their incomes accurately - if the under-ground economy were forced to the surface - the Government could collect an additional \$100 billion a year for the nationl treasury - without raising taxes. States and cities, many in serious financial trouble, would also benefit from collecting previously unpaid income and sales taxes.

How do we create a system to keep cash businesses honest ?? Eliminate cash. That may sound revolutionary, but the exchange of cash for electronic currency is already used in nearly all legitimate international business transactions.

The expansion and application of this concept to domestic transactions would have tremendous benefits, and not just budgetary ones. In addition to forcing cash businesses to report their actual income, it would allow law enforcement agencies to crack down on illicit enterprises.

Think about it. Drug deals, muggings, corruption, businesses concealing their income - they all require cash and secrecy. A monetary system bases solely on electronic currency would leave a trail that would cripple such enterprises.

Here's how it would work. The Government would change the color of the currency and require all old money to be exchanged at the Treasury.

Then, all the new currency would be returned by its owners to the bank of their choice. All banks would be required to open accounts, free of charge, to all depositers. (Banks would surely be delighted to provide this service at it would result in increased deposits.)

We would offer a period of tax amnesty to encourage compliance, but as

a practical matter compliance would be assured because after a certain date all currency would be worthless.

In place of paper money, we would receive new cards - let's call them Americards - each bio-mechanically impregnated with the owner's hand and retina prints to insure virtually foolproof identification.

The Government would supply all homes and businesses, free of charge, with machines, to read the card, certify the holder's identity, and make instantaneous electronic debits and credits. Regardless of what such machines would cost, the Government, with \$100 billion in new revenues and no more printing and mining costs, would come out ahead.

And think of the benefits to the average American. No one would have to write a check again. Bills could be paid electronically from home. Such a system is already available through banks and businesses on a limited, optional basis.

Credit cards would function as they do now. Americard would simply be a way of transferring funds from one account to another, without cash.

For example, on payday, instead of receiving a paycheck, your salary would be electronically transferred into your account. At lunch- time, you would go to your favorite resteraunt - or the local hot dog stand -and instead of paying cash, you'd use your Americard. You'd get a receipt instantly and could get a cumulative record from you bank (or your personal computer) as often as you like.

The benefits would be tremendous. Individuals and businesses would no longer be able to conceal income. All transactions would be recorded in a computerized bank file and would be easy for the I.R.S. to check. Muggers and buglars would be out of business: no one would be carrying cash and stolen property would be difficult to sell because there would be records of all transactions.

Fugitives would be easier to track down, legal judgements easier to enforce, illegal aliens simpler to spot, debtors unable to avoid their responsibilities by skipping town. The census wouln't overlook households.

The Federal Reserve would be better able to follow the economy, helping to stabilize the financial markets. The current series of economic indicators would be replaced by instant access to solid information. And with all income being reported for tax purposes, we could not only balance the budget but actually cut taxes.

Some people might be concerned about possible abuses of civil liberties. But there would be a record of anyone who entered another's account - officials would be granted access only after electronic verification of their hand and retina prints. Civil and criminal penalties for theft of information would be devistatingly severe. Government agencies and prosecutors would be subject to the same Constitutional contraints that currently exist for access to bank information or for the granting of wiretaps.

And there would be no information on the Americard computer that doesn't already exist in other forms today. If anything, our rights to privacy would be more secured with the protections that the Americard would offer.

And besides, I'd like to ask every parent whose child walks to school through a gauntlet of drug dealers, everyone whose home has been robbed, whether they think that their rights have been jeopardized by a system that could solve all these problems ??

Since computer systems occasionally fail, Americard would be contained on several connected secure computers: at the local bank branch, the main bank, the regional office of the Federal Reserve and the Federal Reserve in Washington, D.C. Americard may seem like a drastic approach but its advent is inevitable. In the days of the telegraph and the pony express, who could have imagined that one day there would be a phone on every street corner in Manhattan ??

[Harvey F. Wachsman, a neurosurgeon and lawyer, is president of the American Board of Professional Liability Attorneys.]

[Also noted by Martin Minow, minow@bolt.enet.dec.com]

San Francisco taxes its computer people ... (PGN, <u>RISKS-10.80</u>)

<davidsen@crdos1.crd.ge.com> Fri, 25 Jan 91 15:17:57 EST

Nope, the tax collector is right. People either pay their taxes on time without fail, or they let them go as long as possible, particularly when they are thinking of selling the structure and put the money into either fixup or their pocket.

The people who are behind are probably not going to pay right away, if at all. Rebilling them a little later won't lose anthing, the city charges (I assume) more interest than the banks pay, so better late, actually.

bill davidsen (davidsen@crdos1.crd.GE.COM -or- uunet!crdgw1!crdos1!davidsen)

California's DMV licenses (Re: <u>RISKS-10.79</u>)

The Polymath <hollombe@ttidca.tti.com> 26 Jan 91 03:03:30 GMT

The state of California Dept. of Motor Vehicles (DMV) announced its new format driver's license last week. The license appears to be a standard magnetic stripe (MS) card with the usual driver's license information on the front including the licensee's photograph as a hologram. The DMV claims these licenses will be much harder to fake and forge. They did not say what specific information was on the MS.

The risks of MS cards have been discussed here before. The fact that I'll probably know what's on my license's MS the day I get it should give some idea of how insecure that information is. It takes little more to alter it.

The specifications for MS cards and data are part of a published ANSI/ISO standard. The hardware to build an MS reader/writer can be purchased at Radio Shack.

Further, I can imagine retailers demanding to run my license through their MS readers along with my credit card or to verify a check. I'm not happy about that prospect at all.

The Polymath (aka: Jerry Hollombe, M.A., CDP, aka: hollombe@ttidca.tti.com)

Head Robot Wrangler at Citicorp(+)TTIIllegitimis non3100 Ocean Park Blvd.(213) 450-9111, x2483CarborundumSanta Monica, CA 90405 {rutgers|pyramid|philabs|psivax}!ttidca!hollombe

Kandom Voting IDs and Bogus Votes (Vote by Phone)

<li@helen.oracorp.com> Fri, 25 Jan 91 14:16:48 EST

The lastest RISKS discussed a proposal of "vote by phone" -- registered voters are assigned random numbers as ids, and the ids with the corresponding votes are published afterwards so that voters can verify that their votes are included correctly.

(1) Talking about the use of randomization techniques, one might also want to randomize the ballot papers so that on each individual paper, candidiates are listed in random order. The gains are obvious -- many people just vote for the first name (or the last ?).

(2) PGN rightly pointed out the risk that bogus votes can be inserted because there are no voters who check them. On this front, bogus votes are sometimes useful. David Wheeler and I once thought up the idea of "inserting controled bogus votes" in the following manner.

Each voter is given an id number to vote, but is told that the number is either positive or negative. Suppose there are two candidates, Alice and Bob. If the number is negative, a vote for Alice is actually counted as a vote for Bob. This has the advantage that a third (malicious) party who forces a voter to vote cannot verify (from the published list) if the vote is indeed the desired one. It is easy to generalize to multiple-candidates. An additional advantage is that people can write their numbers on papers. One can steal a number, but won't be sure how to use it (even if I write down +1234567, I could have mentally remembered it to be a negative number. Now I remember 1 bit information, not a long random number).

Of course, there must be some measures to control (and verify ?) the process of counting the ballots. Maybe we are talking about conflicting requirements :-)

Li Gong, ORA Corp., Ithaca, New York. li@oracorp.com

Re: Voting by Phone (<u>RISKS-10.80</u>)

Kathy Vincent <kathy@rbdc.UUCP> Thu, 24 Jan 91 13:47:04 GMT

That's like saying no one can hack your bank account because you have a personal security code. And no numbers are so anonymous that someone so inclined couldn't find out exactly who placed what vote for whom. You may not be so inclined, but some people are -- esp people who want to control outcomes, which is what our secret ballot system is specifically supposed to guard against. If information connecting a person with a vote is stored in such a

manner as to prevent fradulent voting, no matter how fragile the linkage, someone or someones with enough determination can easily find the linkage and exploit it to their own advantage.

Not to mention ... people with the right kind of electronic equipment can sit outside your house and monitor your computer keyboard clicks and know exactly what you're typing. They can monitor your touch-tone phone tones and know exactly what numbers you're dialing. Or what numbers you're using to place your vote -- including your password and anonymous ID number. People with cordless or cellular phones are esp vulnerable. And with the kind of technology that makes caller ID possible, well ...

Ke: Lotus Marketplace (Schumacher, <u>RISKS-10.80</u>)

Samuel Bates <samuel@cs.wisc.edu> Fri, 25 Jan 91 14:03:49 CDT

I would venture to say that the uproar is due to the fact that people heard about the Lotus product, whereas they didn't hear about the others. I would be interested to hear about other ways of getting the same information; if we object to Lotus putting together the product, then we should object to other companies doing the same. If you can get names of companies that produce the information, I would like to know them. Barring that, will you tell me the names of the academics with whom you spoke?

Samuel Bates samuel@cs.wisc.edu University of Wisconsin-Madison

Ke: Superloo (Campin, <u>RISKS-10.80</u>)

Lars-Henrik Eriksson <lhe@sics.se> Sat, 26 Jan 91 19:37:57 GMT

There is an obvious risk here. In fact, I have read a newspaper report (although it was several years ago so I can't give any sources), that this "disinfecting cycle" once started while a girl was still inside. She later died because of lung damages after having inhaled the disinfectant fluid.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263 S-164 28 KISTA, SWEDEN +46 8 752 15 09



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Ke: Patriot Missile (Agre, <u>RISKS-10.81</u>)

Dave Parnas <parnas@qucis.queensu.ca> Mon, 28 Jan 91 23:21:58 EST

Phil Agre <phila@cogs.sussex.ac.uk> asked for comments about the "Patriot" missiles. There seem to be people around who are trying to exploit events in the Gulf War to revive SDI. Let's look at his remarks one at a time.

>"The Patriot missiles genuinely seem to be working well, at least in the >desert environment."

Actually, we have very little information about how well they are working. We know that they have had some successes and some failures but we have no idea how many Patriot's have been fired for each SCUD shot down.

> Yet a few years ago the Patriot was the very prototype of the incompetent> high-tech military development program. Its testing in particular came in for

>congressional ridicule. What happened?

Among other things, it has been given a particularly easy job. It was originally developed as an anti-aircraft system, not an ABM system. In many ways the job of a terminal phase (point defense) ABM system (for incoming missiles or warheads in unpowered flight) is much simpler than the anti-aircraft task for which Patriot was first developed. Aircraft can take evasive action and use sophisticated devices to fool systems like Patriot. Older missiles such as the SCUD can do neither. I suspect that the Patriot is still not very effective on its original target, manned aircraft. The SCUD is an ideal target for the Patriot.

As far as I can determine the key to the Patriot is the launcher, which has a sophisticated Phased Array Radar that can track incoming objects, backed up by a computer that can predict the future path of the object (assuming that it is not powered or steered). This is a rather simple job. The Patriot has an operator to determine whether an object being tracked is friend or foe and designate a target. The Patriot missile itself is launched on a path that will intercept the path of the incoming missile (another simple application of physics) and has a very simple homing system that is effective when (and if) it gets near its target. Were the target missile to change course drastically after launch, the Patriot missile would end up somewhere else. Some reports indicate that some Patriots have missed their targets and ended up where they did damage to the buildings that they were supposed to protect. (These are unconfirmed reports.)

>According to its manufacturer and to various other experts quoted in the >press, its software was greatly improved through the application of software >technology developed for SDI.

The design and production phase of the Patriot was completed in 1980, and the missile went into operational status in late 1984. Flight tests of the Patriot started in 1974. The development and manufacture tooling stage of the Patriot was completed in 1980, the year before Reagan took office. The SDI program was not announced until 1983. There was no SDI software technology to be applied to Patriot. In fact, I believe the reverse was true. SDIO funded Raytheon to see if the Patriot ideas could be used for the terminal phase components of SDI. If there was technology transfer, must have been from Patriot to SDI. Remember that SDI funds were to be used for "research" on the space-based shield; they were not to be used for improving other weapons.

>These experts regard the success of the Patriot as evidence that the >SDI's software nay-sayers were wrong.

Those experts had better go back and read what we "software nay-sayers" actually said. The objections that were raised were to the space based aspects of the system. I, and others, repeatedly said that the only place where something could be done was the terminal phase for the defense of important (hardened) targets. Terminal phase defense systems like Patriot can operate without the elaborate communication and synchronization that was envisaged for SDI and do not have to automate the decisions that would have to be automated for the space-based system. Terminal defense systems can have an operator who makes decisions that would have had to be automated in the space-based system. The range of terminal defense systems is rather limited and they cannot prevent

the warheads of the incoming missile from detonating if intercepted. For SCUD missiles that carry conventional armaments this is not a serious problem. For the threat portrayed by SDI supporters it was a fatal weakness. Patriot is subject to all the known limitations of terminal phase defense systems. For example, the maximum range is reputed to be 70km and the effective range is reduced if the launcher is not near the projected impact point.

We should never forget that the Patriot was about 19 years in development. (Remember former President Reagan's generous offer not to deploy SDI for 7 years!) The SCUD was first deployed about 1965 - Patriot about 19 years later. All RISKS readers should think about the advances that we have seen in 19 years. It should come as no surprise that the Patriot can sometimes destroy missiles that were deployed when its development began. The interesting question is what it would do against aircraft and modern weapons.

Dave

Patriots: Reprogramming, SDI implications

Nathaniel Borenstein <nsb@thumper.bellcore.com> Mon, 28 Jan 1991 15:16:04 -0500 (EST)

I heard this weekend on NPR that American & Israeli technicians are furiously working to reprogram the Patriots to be "more intelligent about people on the ground." It seems that nothing in the Patriot's programming informs it about the population (or lack thereof) in the area. The NPR report was unclear on what the differential actions would be, but I presume that it might have options regarding the moment of interception, and is being reprogrammed to favor intercepting when not directly over a populated area. Aside from being amazed that this was never taken into account in the first place, I'm awestruck that they're willing to reprogram the Patriot -- which seems, after all, to basically work -- right in the middle of the war! I know I feel like I'm living dangerously even when I install a new binary in peacetime...

On the subject of "Does Patriot prove SDI could work?" I think the answer is a clear and resounding no. First of all, the Patriots can't even hit all the SCUD missiles. Letting 1 of every 10 SCUDs through is a big success, but letting 1 of 10 Soviet nuclear missiles in would be a disaster. Second, the SCUD is a relatively slow missile that follows a fixed trajectory; it would be useless against anything that can take evasive action, such as a Cruise missile, and you'd probably need some sort of AI-like techniques to predict the future trajectory of a Cruise taking evasive action. Finally, I heard an air force officer explaining on CNN the other day that the Patriots may never again be as useful as they are being in this war, because "now that their capabilities are known, it will be trivial to make the next generation of missiles able to fool them. Basically, in this game all the cards are stacked in favor of the offense." In other words, we're very lucky that the Patriots are so well suited to the current situation, but we'd be foolish to extrapolate wildly to future situations, and particularly to SDI.

Re: Patriot (RISKS-10.81)

Phil R. Karn <karn@thumper.bellcore.com> Mon, 28 Jan 91 20:24:19 EST

Ever since the first successful Patriot intercept over Saudi Arabia, I began waiting for the SDI crowd to being crowing. I didn't have to wait long - Louis Rukeyser on PBS's Wall Street Week last Friday was one notable example of engaging mouth with brain in neutral.

But no reputable critic of SDI ever said that a system like the Patriot could NEVER hit missiles fired singly or in small volleys that target relatively small areas, carry conventional high explosive warheads, and lack some fairly obvious countermeasures.

Yet despite the relatively easy targets presented by the Iraqi SCUDs there have already been quite a few failures of the Patriot to destroy them, and several cases where the Patriots have themselves apparently caused damage to the cities they are supposedly protecting. I wouldn't exactly use the phrase "genuinely seem to be working well" when night after night I see TV footage of missiles (incoming SCUDs and/or errant Patriots) producing unmistakable explosions when they hit the ground in Saudi Arabia and Israel.

If the SCUDs launched at Israel over the past two weeks had been carrying nuclear weapons (which is, after all, the original SDI scenario), northern Israel would now be a smoking ruin -- Patriots or no Patriots. Even the Pentagon admits Patriots are of little use against SCUDs armed with chemical warheads since they would merely disperse the chemical over the target. [...]

Phil

Ke: Patriot missiles

Hans Mulder <hansm@cs.kun.nl> Tue, 29 Jan 91 18:16:26 +0100

In Risks 10.81 Phil Agre writes:

> The Patriot missiles genuinely seem to be working well, at least in the > desert environment.

Actually, a bug was discovered last week. Apparently, Patriot launchers can operate in two modes: fully automatic and human-in-the-loop. They have been exercised in human-in-the-loop mode for several years now, and work rather accurately that way. But the Patriot launchers defending cities in Isreal and Saudi Arabia are currently running in fully automatic mode, primarily on the ground that they can react a few seconds faster that way. In contrast, the Patriot launchers defending Incirlik Air Base near Ardana, Turkey, reverted to running in human-in-the-loop mode after it was discovered that a bug in fully automatic mode causes the machine to occasionally launch two missiles for no reason (they are always launched in pairs -- presumably because they are so reliable :-}).

A Ministry of Defense spokesperson explained: ``We can't afford to waste these missiles: they cost \$600,000 a piece.'' I haven't seen such a thorough risk assessment for years...

Hans Mulder hansm@cs.kun.nl

Ke: <u>Risks 10.81</u> (Patriot missiles and electronic "cash")

&arl.Kluge@G.GP.CS.CMU.EDU> Mon, 28 Jan 1991 21:13-EST

1) No one, but no one, that I am aware of ever seriously suggested that it was impossible to construct software to do terminal interception of ballistic objects. That is a gross distortion of the arguments over SDI software. The idea that the success of the Patriot has any impact (sic) on the issues involved is false.

2) I have seen the electronic "cash" proposal before, and yes these people are serious. My basic philosophy is that the government should have to justify to me why I ought allow them to keep data on me. The idea behind this proposal is that I somehow have to justify to the government why they shouldn't have data on me -- the old "if you have nothing to hide, it shouldn't bother you" argument. Given what we know the government is capable of (remember J. Edgar Hoover, or Nixon's "dirty tricks" squad?) to try to reassure people by saying "Governmental agencies...would be subject to the same Constitutional constrints that currently exist...for the granting of wiretaps" is a joke. Almost makes me want to buy a gun and join the NRA.

Karl Kluge (kck@g.cs.cmu.edu)

Ke: Electronic cash completely replacing cash (<u>RISKS-10.81</u>)

David Lamb <dalamb@umiacs.UMD.EDU> Mon, 28 Jan 91 15:39:10 -0500

Hmm. I know this isn't misc.legal or talk.politics, but... In addition to the obvious RISKS reasons to resist this one, I imagine any serious proposal would get tremendous opposition from fundamentalist Christians, demanding (at least) an exemption for religious reasons. There's a prophecy in Revelations about "the mark of the Beast" without which one could neither buy or sell. There was tremendous furor about Social Security numbers when they were first introduced, from the same group, for the same reason. This proposal is a lot more like the Mark than SSN's were.

And of course, one exemption would breed others.

David Alex Lamb

K Re: Electronic cash completely replacing cash (`witt', <u>RISKS-10.81</u>)

Larry Nathanson <lan@bucsf.bu.edu> 28 Jan 91 22:37:57 GMT

> If all the people who do business in cash were forced to
 >report their incomes accurately - if the under-ground economy were
 >forced to the surface - the Government could collect an additional
 >\$100 billion a year for the nation! treasury - without raising taxes.

How is the author so sure of his figures, if this is money that has not been reported?

How do we create a system to keep cash businesses honest ??
 >Eliminate cash. That may sound revolutionary, but the exchange of
 >cash for electronic currency is already used in nearly all legitimate
 >international business transactions.

Define "honest". If every store complied with every last OSHA regulation, most small businesses couldn't afford to stay in business. Sometimes small businesses skirt the rules slightly so as to be able to stay in business. There won't be much of an increase in tax revenue, if the letter of the law is enforced so strongly that no business can survive.

> Think about it. Drug deals, muggings, corruption, businesses
 > concealing their income - they all require cash and secrecy. A
 > monetary system bases solely on electronic currency would leave a
 > trail that would cripple such enterprises.

Just because the listed illegal acts all require secrecy, does not mean that all secret acts are illegal. If I share an account with my wife, and we both have instant access to every last dime, I can't throw her a surprise party or really be at the bar drinking, when I told her I was at the office. What about minors? Do they have their own card? Do their parents get to see their accounts? Or are they just not allowed to have money?

> Then, all the new currency would be returned by its owners to >the bank of their choice. All banks would be required to open >accounts, free of charge, to all depositers. (Banks would surely be >delighted to provide this service at it would result in increased >deposits.)

Tell that to my bank. I get hit for around \$8 a month just to have an account. It costs money to maintain the information. If everything was completely dependent on this system, as the article states, then it would cost more to maintain the information. No bank in their right mind would let me keep a \$20 account without a monthly.

In place of paper money, we would receive new cards - let's
 call them Americards - each bio-mechanically impregnated with the
 owner's hand and retina prints to insure virtually foolproof
 identification.

What about those who don't have hands? Or retinas? Or neither? If I buy a

pair of socks, I have to be fingerprinted, and put my eye to a machine? (BTW-great way to spread conjunctivitis)

The Government would supply all homes and businesses, free of
 charge, with machines, to read the card, certify the holder's
 identity, and make instantaneous electronic debits and credits.
 Regardless of what such machines would cost, the Government, with \$100
 billion in new revenues and no more printing and mining costs, would
 come out ahead.

Hmmm.. a combination MS card reader, full hand finger print analyzer, retina scanner, computer, and modem, supplied to every individual that wants one. This is supposed to save money over green ink on white paper?

And think of the benefits to the average American. No one
 would have to write a check again. Bills could be paid electronically
 from home. Such a system is already available through banks and
 businesses on a limited, optional basis.

And that's the way it should be. On an optional basis. What if I WANT to write a check? What if I'm going to mail a check to someone, so that by the time it gets there, it will be payday, and I'll have money in my account? Instantaneously paying bills from home is great, IF you want to pay them that way.

For example, on payday, instead of receiving a paycheck, your
 salary would be electronically transferred into your account. At
 lunch- time, you would go to your favorite resteraunt - or the local
 hot dog stand -and instead of paying cash, you'd use your Americard.
 You'd get a receipt instantly and could get a cumulative record from
 you bank (or your personal computer) as often as you like.

And the hot dog vendor can see how much money I've got in my account? Every last hot pretzel vendor on the streets of NYC is going to have a MS card reader/retina scanner/fingerprint analyzer? (Not to mention a generator to keep it running) Some of these guys can't afford the wood to burn under the pretzels!

> The benefits would be tremendous. Individuals and businesses
 >would no longer be able to conceal income. All transactions would be
 >recorded in a computerized bank file and would be easy for the I.R.S.
 >to check. Muggers and buglars would be out of business: no one would
 >be carrying cash and stolen property would be difficult to sell
 >because there would be records of all transactions.

Money purely man's invention. If people can't get access to 'real' money, then they will find something else of value, and trade it instead. Gold, Silver, Platinum, and everything else of value would have to be banned. Not to mention barter. This wouldn't even put a dent in illegal activities. But on the other hand, Joe's wife could notice that he bought a 24 pack of condoms, the day after she left on a business trip.

Fugitives would be easier to track down, legal judgements
 >easier to enforce, illegal aliens simpler to spot, debtors unable to

>avoid their responsibilities by skipping town. The census wouln't >overlook households.

I'd say the odds on it magically reducing tooth decay are better than the odds on it fixing any one of the above problems.

And there would be no information on the Americard computer
 that doesn't already exist in other forms today. If anything, our
 rights to privacy would be more secured with the protections that the
 Americard would offer.

I fail to see the logic underlying that statement.

And besides, I'd like to ask every parent whose child walks to
 school through a gauntlet of drug dealers, everyone whose home has
 been robbed, whether they think that their rights have been
 jeopardized by a system that could solve all these problems ??

In other words, in order to prevent crime, we should radically change the economic structure of our country. Instead of Americards, how about just switching to communism! In the Soviet Union only drug problem is alcohol, and the muggers are shot in the streets. It would be a LOT cheaper just to elect the communist party than to muck around with all this technology stuff. Maybe there are some things that Americans hold more dear (like freedom and privacy) than things even like safety.

Since computer systems occasionally fail, Americard would be
 contained on several connected secure computers: at the local bank
 branch, the main bank, the regional office of the Federal Reserve and
 the Federal Reserve in Washington, D.C.

And making the system more complex would tend to reduce problems and increase security?

> Americard may seem like a drastic approach but its advent is >inevitable. In the days of the telegraph and the pony express, who >could have imagined that one day there would be a phone on every >street corner in Manhattan ??

Poor analogy. There are many inventions and ideas that never made it off the drawing board. This will be another.

Larry Nathanson . 726 Comm Av #5J . Boston, MA 02215 . 617 266 7419

Ke: Electronic cash completely replacing cash (`witt', <u>RISKS-10.81</u>)

Randal L. Schwartz <merlyn@iwarp.intel.com> Mon, 28 Jan 91 15:49:21 PST

[...] I'd hate to see this system in place. I'm not a luddite, but replacing moveable tokens for ones and zeroes that are necessarily manufactured and replicated at will is opening up a whole bunch of issues all at once. We don't

have the authorization/authentication technology far enough along and cheap enough to do this on a national scale yet.

And, are you really going to give every man, woman, and child a smartcard? "Here's your allowance junior. Oops! The cardreader is broke. Well, I guess you're not getting one today." And what about the gazillions of vending machines out there? Are you going to make those invalid overnight?

A suggestion I had seen was that there'd be small "currency" valid for amounts under, say, \$100. Banks (or corner vending machines) would provide for transfers between your smartcard and some "currency".

I think we're getting closer to this compromise forced not by government mandate, but by economics. Bills over \$100 haven't been printed for quite some time, because most legitimate uses of those bills have been replaced with EFT. I'm using cash less and less each day. I pay nearly all of my daily expenses with my Visa card. In fact, the local Burger King and Seven-Eleven stores take Visa now! I write checks to pay my bills through the mail, although many pay-by-phone services exist so that I wouldn't even have to do that.

And not one part of this is by government mandate. Economics have pushed the gradual phase-in of the cashless society. And it's happening quite gradually and rather nicely, thank you.

Just another cash-kinda-guy,

Randal L. Schwartz, Stonehenge Consulting Services (503)777-0095 merlyn@iwarp.intel.com ...!any-MX-mailer-like-uunet!iwarp.intel.com!merlyn

✓ Electronic cash completely replacing cash (<u>RISKS-10.81</u>)

K. M. Sandberg <sandberg@ipla01.hac.com> 28 Jan 91 21:16:18 GMT

The worst part about this is that I am sure that the author believes what is said, yet fails to understand the risks involved. True, it would get more tax dollars, but at an unknown cost for all the machines and networks to make it work. What do you do if you lose your card since nobody will trust you without it? With cash at least you can put some aside in case of emergency, but with only a card that may decide to not work it is all or nothing.

It also assumes the the barter system does not exist, after all who would exchange items for work. Unless you then take inventory of all the items that a person bought, just to make sure.

Of course the line of "if you are honest, why should it bother you" is bound to come up. This means that "honest" people would not mind having cameras watching them all the time since it would cut down on crime, then you could tatto everyone so that there is no doubt about identification. And so it goes, welcome to 1984 by Orwell.

Was this in the editorial or opinion section at least? Also what does it take

to get people to think about what they are saying, or to just plain think?

Kemasa

🗡 Americard...

Peter da Silva <peter@taronga.hackercorp.com> Tue, 29 Jan 1991 00:46:28 GMT

> Think about it. Drug deals, muggings, corruption, businesses
 > concealing their income - they all require cash and secrecy. A monetary
 > system bases solely on electronic currency would leave a trail that would
 > cripple such enterprises.

And, of course, let others flower. How well would a cashless economy have prevented the S&L scandal? And, of course, the government would have to call in all the precious metals again. This would just make it easier for the rich... with easily liquifiable assets in the form of stocks, bonds, real estate, and so on... at the expense of the poor and middle class.

And that's without considering the possibility of fraud in the system itself!

🗡 Re: Abolish Cash

Richard Keeney <keeney@vixvax.mgi.com> Tue, 29 Jan 1991 00:11:30 CST

When I read the artical "Abolish Cash" by Harvey F. Wachsman, "The Government" appears to be the only safegard in his proposed system. Many people would agree with me when I bring up the point that we still have not devised a good method of completely safeguarding ourselves from the various forms of government that are necessary to run our society. A system where the appropriate legislative body has such absolute control over trade and enterprise would seriously undermine the population's ability to remove such a body from power when they no longer agree with that body's policies or activities. I would assert that "cash" provides a significant safeguard of our right to freely assert our political views, especially in the face of disagreement from those currently in power.

I will go even further and point out that such a legislative body would find it almost impossible to resist making full use of the level of control offered by such a system, and would certainly find many innovative ways to make us regret giving them so much control. There are many historical examples of how even the best intentioned use of legislative power can go bad. Not only do we have no reason to trust "The Government" with such a system, but we have many reasons to mistrust them.

Another weakness of such a system that I would like to point out relates to the inability of such a system to deal with all the seemingly small but necessary transactions required to "grease" the machine to make things move smoothely. I can imagine that people would become obsessed with every little penny. When

you have to take the trouble to make an official "transaction", people will become less generous with things like gratuities, informal loans, small gifts, etc.

Such a system would be very cruel (perhaps even to the point of violating our constitutional right to be free from cruel and unusual punishment) to somebody who is denied access to their money due to a lost or damaged card, an error, or red tape. One day everything would seem fine, and the next, wham! "I am sorry sir, but we cannot accept your Americard due to a hold placed by agency Red_Tape_Is_Us relating to a delinquent payment of \$0.39. By the way sir, you can clear that up with them on Mondays between 2:00 and 3:00 PM (excepting national holidays of course) if you fill out form 55-A-1-55-92194 in triplicate and have a note from your mom."

I would also like to point out one area that would be very similar to credit cards that would require additional thinking. What happens when there is a dispute over a charge between a merchant and a customer? Who would have the onus of proof? What about when a merchant has to have a person's account number to post a running series of transactions as in the case of a hotel, for example? It would be tough to imagine Uncle Sam eating those disputed amounts like credit card companies often do to keep the good will of both the card holder and the merchant. Truth in advertising would also continue to be a problem. How do you know what charge will appear on your card when you put it into a vending machine or give the number to some mail order merchant?

Finally, I think "Americard" may already be registered as a trademark by somebody (Ameribank sticks in my head).

Richard A. Keeney, Senior Software Engineer, Management Graphics, Inc., 1401 East 79th Street #6, Bloomington, MN, 55425 Phone: +1-612-851-6126



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Olivier M.J. Crepin-Leblond" <MEEB37@vaxa.cc.imperial.ac.uk> Tue, 29 Jan 91 14:25 BST

Following is a translation of a short article published in a French newspaper "Le Figaro", on 21st January 1991. It was part of a special supplement describing the new electronic weapon systems the allies are currently using.

Electronic navigation systems are now so advanced that the pilot of a fighter airplane is not obliged to play an active role during the flying phase. The computer is in fact a better pilot in sorties involving penetration of enemy territory by flying at very low altitude (under the sensitive radar zones). It is not prone to tiredness, and much better at avoiding obstacles: it is therefore possible to fly at supersonic speed (< 1000 km/h) in a hilly region, whilst constantly being at an altitude of 15 metres from the ground. This is

very reliable, since the sensors of the airplane constantly provide data which the navigation systems computer uses.

Unfortunately, the actual pilots cannot stand this type of passive flight. Not because by vanity, but because they tend to get sick: the U.S. Air Force has found out during experimental missions that even the best and toughest of pilots gets sea-sick after a few minutes when submitted to accelerations and bearing changes that he did not generate himself.

This is so serious that when some pilots arrived at the target site, they had lost all faculties of analysis, and as a result the U.S. Air Force has decided to abandon at least partially the concept of automated piloting for very low altitude flights. "

Olivier M.J. Crepin-Leblond, Elec. Eng., Imperial College London, UK.

Marcadcast local area networks are a'comin

&om.Lane@G.GP.CS.CMU.EDU> Tue, 29 Jan 91 11:30:10 EST

Today's New York Times states (on page two of the business section) that Apple has filed with the FCC to reserve radio bandwidth for use in wireless local area networks. Instead of running LAN cable all around your building, you put low-power transmitter/receivers in all your machines, and away you go. The assigned bandwidth would be used by all comers on a first come, first served basis within each area, much as cordless phones or garage door openers are now. They estimate 150ft as the useful radius of communication; data rates would be the same as wired LANs (10Mb/sec or so).

The risks should be pretty obvious to readers of this digest. Somebody in the next building could eavesdrop on your traffic, or actively connect into your net, with NO special hardware. I sure hope Apple is at least planning to encrypt the packets---no mention of this, or of any security concerns, in the article. (But if they are going to support 10Mb/sec data rates, the encryption would have to be fairly weak, methinks.)

If I ran a corporate network, I wouldn't touch this with a 10-foot pole.

tom lane

Ke: Risks in forensic use of dental and medical records

Jim Purtilo <purtilo@cs.UMD.EDU> Mon, 28 Jan 91 15:26:31 -0500

I can offer first-hand experiences concerning use of technology in forensics. Some colleagues and I have developed software systems to help manage forensic information `in the field' following a mass casualty disaster. Initially we focused upon dental information, where the goals are to capture both antemortem and postmortem records rapidly, then suggest possible matches between them. Based upon suggestions from the software, an expert would take the time only to perform an autopsy (in order to confirm the match) once enough confidence had been built up by the software that the match was likely. Previously, only paper records were kept; matches were based upon having medical examiners pick up a file folder of raw records, and then walk down a long row of human remains, comparing each in turn until a possible match was found. With our software, both goals are attained:

- 1. Some amount of organization was brought to raw data that begins to gush forth after a tragedy (dentists employ many recording schemes, most of them conflicting, it seems).
- 2. The heuristic we developed for suggesting matches works. Our first suggestion for a possible match has proven to be correct better than 95% of the time, based upon analysis of records that have been made available to us following previous air disasters.

So much for the advertising. Now for the nitty gritty. The only way we can obtain this success is by *ignoring* much of the key information that an expert would use to help make a positive identification! Earlier versions of our program attempted to consider detailed information about such things as root canals, the quality of tooth enamel (hypoplasia, abrasions, mottled), and shape of incisors. The program was magnificently successful when used with quality information. However, our testing showed that there is almost no quality information to be had in the first place. Dentists (some!) will charge for work not done, or will mark the wrong tooth on paper records when in a hurry to get to the next patient (off by one, or right index from wrong side of mouth). They will mark down the wrong type of filling material. Or they won't update a patent's records if they find new work done there by someone else (say, the patient was on the road, needed a quick filling by someone near at hand). And so on. Never mind the problems that any program will have should you send out for the records of "Jane and John Doe", only to find Jane answers the phone, but John's secretary is missing...

Next, the transcription problem. Lots of data, with diverse formats and inconsistent attention to details, cannot be accurately transcribed by assistants conscripted by airlines (or local ME office, or whatever).

With experiments, we were able to find a choice of parameters that is least likely to be screwed up in the original antemortem form, is sufficient to get us very close in suggested matches, and yet is simple enough that a spreadsheet editor can let users enter all the material on one screen. By giving up the urge to use all the data and be *exact*, we were able to find a solution that got very close. In this case, this is sufficient to guide expert users, who will then make very good use of their time (confirming matches, not investing time looking for them).

In summary, Sherizen's observation is correct: the key problem is obtaining accurate information in the first place (i.e., we have rediscovered GIGO). The key engineering problem, therefore, is anticipating common error modes and adapting our technology accordingly.

Jim Purtilo, Computer Science Department, University of Maryland

Patriots

"Clifford Johnson" <A.CJJ@Forsythe.Stanford.EDU> Tue, 29 Jan 91 10:57:45 PST

There was an accidental Patriot launch in Turkey of two Patriots against aircraft returning from Iraq. Four aircraft took evasive action, and all esacped. Although the system was in anti-ballistic (vs. anti-aircraft) mode, this does show the Patriot may be useless against anything other than predictably moving hunks of metal, and that automatic launch on warning is as dangerous as we thought.

Ke: Patriot Missile

wegeng@arisia.xerox.com &onald_L._Wegeng.henr801c@xerox.com> Tue, 29 Jan 1991 10:47:13 PST

Dave Parnas writes in <u>RISKS 10.82</u>: > There was no SDI software technology to be applied to Patriot.

Today I spoke with someone who works in an engineering capacity with a US Army guided missile group (I didn't ask if my source minded being quoted, so I won't be more specific). According to my source, the sensors that are currently being used on Patriot missiles to track BMs were developed as part of the SDI program (recall that the Patriot was originally an anti-aircraft system, and thus used different sensors). The first test of these new sensors on a Patriot took place about six months ago at White Sands. So while the Patriot itself is not based on SDI technology, the sensors that it uses to track BMs are based on SDI technology.

Don Wegeng

Ke: Patriots, and whats under them at intercept.

Ed Wright <edw@sequent.uucp> 29 Jan 91 18:48:59 GMT

Some years back I was stationed with HHB 45th Arty (AD) a Nike Hercules unit. 45th ADA was located in Arlington Heights II, a suburb of Chicago at the time. The Herc had a high explosive warhead, but could also be fitted with one of several nuclear warheads. Contemplating the effects of a nuclear blast over say Northfield (a northern suburd of Chicago) and being willing to question authority I posed to my superior the question "What good does it do to shoot down a Russian bomber with a missle that will destroy the town under it ?" and the reply was "Well son what would you rather have: ## kilotons over Evanston, or 10 to 50 megatons over the loop ?" Now at the time it almost made sense, 10 to 50 mt over the loop would sure negate the suburbs, and ## kt in the burbs would only cause significant damage to the loop area. Please note the key word is almost. I have no doubt that the same mindset is in use today and the question has got to be: "Well son, would you rather have big burning fragments of Patriot and Scud over the burbs or a Scud downtown ?" {Could that be Scud or Scud Lite ? :-) } I sure as hell don't have the answer. Ed Wright

Ke: Random Voting IDs and Bogus Votes (Vote by Phone)

Raymond Chen <raymond@math.berkeley.edu> Mon, 28 Jan 91 11:34:09 PST

In <<u>RISKS DIGEST 10.81</u>> li@helen.oracorp.com proposed a partial precaution against bogus-vote insertion, namely that some votes be tagged `negative', meaning that the votes cast are really reversed. I leave the security and sociological consequences to more qualified folk.

I address the following claim:

>(even if I write down +1234567, I could have >mentally remembered it to be a negative number. Now I remember 1 bit >information, not a long random number).

I wouldn't trust the public's ability to remember a single bit of information. Indeed, even I have trouble remember whether the my front door is locked or unlocked when the handle is in the vertical or horizontal position, and this is a door I lock every day.

Voting by phone and buying votes

Colin Plumb <ccplumb@rose.uwaterloo.ca> Mon, 28 Jan 91 17:29:46 EST

This is out of high school history, but fortunately that isn't too far in the past for me:

The old technique for buying votes had a person watching on the way from the voting booth to the ballot box. You had to unfold your ballot and show them a correctly marked ballot, then go and drop it in the box. Then you got yor \$5 (or whatever it was). If not, you got a visit from some large guys.

Politics is almost the definitive dirty activity. We need a very foolproof way to prevent influence where we don't want it. I'm not implying that anyone today would engage in widespread abuse, but blatant vote-buying is not too long in Canada's history, at least (I don't know about the U.S.), and it could return in 25 years.

To be secure against bribery and intimidation of individual voters, it must not be possible for A to prove to B that he did or did not vote for B. (Well, if *nobody* in A's district voted for B, then B has some idea, but...)

This is why I like the current method of constructing a human-readable ballot and placing it in a box. Recounts are possible, the voter can clearly see what they're doing, and ensuring that there are initially no ballots in the box and that each voter places at most one ballot in the box is relatively easy and can be done by several witnesses. It's not impossible to abuse, but it requires a large conspiracy. Will these voting by phone techniques prevent me from signing up a few hundred drunks, having them vote from a telephone I supply, with me listening on an extension, and giving them each a bottle of rum afterwards? In a marginal constituency, this could make a difference.

-Colin

✓ Call for Papers -- 7th Computer Security Applications Conference

<faigin@aerospace.aero.org> Mon, 28 Jan 91 09:31:11 PST

CALL FOR PAPERS AND PARTICIPATION

Seventh Annual Computer Security Applications Conference December 2-6, 1991 San Antonio, Texas

The Conference. Operational requirements for civil, military, and commercial systems increasingly stress the necessity for information to be readily accessible. The Computer Security Act of 1987 requires that all Federal agencies take certain actions to improve the security and privacy provided by federal computer systems. Accomplishing both operational and security requirements requires the application of the maturing technology of integrated information security to new and existing systems throughout their life cycle. This conference will explore technology applications for both civil and military systems; the hardware and software tools and techniques being developed to satisfy system requirements; and specific examples of systems applications and implementations. Security policy issues and standards will also be covered during this five day conference.

Papers and Tutorials. Technical papers and tutorials that address the application of integrated information security technologies in the civil, defense, and commercial environments are solicited. Original research, analyses and approaches for defining the computer security issues and problems identified in the Conference's interest areas; secure systems in use or development; methodological approaches for analyzing the scope and nature of integrated information security issues; and potential solutions are of particular interest. A prize of \$500, plus expenses paid to attend the conference, will be awarded for the best paper written by a student. For details contact Ravi Sandhu at the address below.

INSTRUCTIONS TO AUTHORS: Send five copies of your paper or panel proposal to Ann Marmor-Squires, Program Chairman, at the address given below. We provide "blind" refereeing; put names and affiliations of authors on a separate cover page only. It is a condition of acceptance that manuscripts submitted have not been previously published. Papers that have been accepted for presentation at other conferences should not be submitted. Tutorial proposals should be sent to Daniel Faigin at the address given below. Papers and tutorial proposals must be received by May 17, 1991. Authors will be required to certify prior to June 19, 1991, that any and all necessary clearances for publication have been obtained, that they will be represented at the conference to deliver the paper, and that the paper has not been accepted elsewhere. Authors will be notified of acceptance by July 29, 1991. Camera ready copies are due not later than September 18, 1991. Material should be sent to:

Ann Marmor-SquiresDaniel FaiginTechnical Program ChairTutorial Program ChairTRW Systems DivisionThe Aerospace Corporation2751 Prosperity Ave.P.O. Box 92957, MS M1/055Fairfax, VA 22031Los Angeles, CA 90009-2957(703) 876-8161(213) 336-8228marmor@a.isi.edufaigin@aerospace.aero.org

Ravi Sandhu, Student Paper Award, George Mason Univ., ISSE Dept., Fairfax, VA 22030-4444, (703) 764-4663 sandhu@gmuvax2.gmu.edu

Areas of Interest Include: Advanced Architectures, C3I Systems, Trusted DBMSs and Operating Systems, Public Law 100-235, Networks and Open Systems, Software Safety, Policy and Management Issues, Risk/Threat Assessments, State-of-the-Art Trusted Products, Electronic Document Interchange and Modeling Applicability, Certification, Evaluation and Accreditation, Current and Future Trusted Systems Technology, Reviewers and Prospective Conference Committee Members.

Anyone interested in participating as a reviewer of the submitted papers, please contact Ann Marmor-Squires at the address given above. Those interested in becoming members of the conference committee should contact Dr. Ronald Gove at the address below.

For more information or to receive future mailings, please contact the following at:

Diana Akers
Publicity Chair
The MITRE Corporation
7525 Colshire Dr.
McLean, VA 22102
703) 883-5907
akers@mitre.org

Victoria Ashby, Publication Chair, The MITRE Corporation, 7525 Colshire Dr., McLean, VA 22102 (703) 883-6368 ashby@mitre.org

Call for papers, Theorem provers in circuit design

&ictoria.Stavridou@prg.oxford.ac.uk> Fri, 25 Jan 91 15:00:32 GMT

> CALL FOR PAPERS INTERNATIONAL CONFERENCE ON

THEOREM PROVERS IN CIRCUIT DESIGN: THEORY, PRACTICE AND EXPERIENCE

NIJMEGEN, THE NETHERLANDS, 22-24 JUNE, 1992

FOCUS AND OBJECTIVES

Formal methods are increasingly seen as important in the design of digital systems. The use of these techniques in practice is often regarded as being strongly dependent on the support of appropriate mechanized theorem proving tools. The purpose of this conference is to provide a forum for discussing the role of theorem provers in the design of digital systems. The objective is to cover all relevant aspects of work in the field, including original research as well as case studies and other practical experiments with new or established tools.

The primary focus will be on the ways in which formal methods are supported by theorem proving tools, rather than on the theoretical foundations of formalisms and design methods. The topics of interest include the philosophy behind such tools, their design and development, their evolution, and their evaluation through use. Of equal importance is the migration path of a theorem proving tool and the associated technology into current digital engineering practice.

The intended audience includes workers in the field of hardware verification as well as practising digital designers.

TUTORIALS

It is intended that the conference will address, among other issues, practical questions such as:

Why use a theorem prover? Which theorem prover should I use? When should I use it? How should I use it?

To enhance this aspect of the proceedings, the working sessions will be complemented by tutorials on a variety of theorem proving tools and associated topics. A Tutorials Chair has been established to ensure that a wide range of systems are represented and to underline the importance that is placed on the matter.

PROGRAMME AND PROCEEDINGS

The conference programme will start with a day of tutorials and demonstrations, followed by two days of presentations by contributing authors. The programme will also include invited lectures by three prominent researchers in the field of machine-assisted verification. The invited speakers are:

Mike Gordon, University of Cambridge.

Warren Hunt, Computational Logic Inc. Dave Musser, Rensselaer Polytechnic Inst.

A digest of papers will be made available to participants at the conference and the proceedings will be published after the conference.

ORGANIZATION

The conference is organized by the Computer and Communications Systems Group of the University of Nijmegen, the Netherlands. The conference organizers are:

General Chair: Raymond Boute, University of Nijmegen.

Programme Chair: Victoria Stavridou, University of London.

Tutorials Chair: Tom Melham, University of Cambridge.

Local Arrangements Chair: Huub van Thienen, University of Nijmegen.

PROGRAMME COMMITTEE

The programme committee includes:

Albert Camilleri (HP Labs, UK) Luc Claesen (IMEC, Belgium) Ed Clarke (CMU, USA) Mike Fourman (Edinburgh Univ., UK) Joseph Goguen (Oxford Univ., UK) Allen Goldberg (Kestrel Institute, USA) Keith Hanna (Univ. of Kent, UK) Warren Hunt (CLInc, USA) Jeff Joyce (UBC, Canada) Deepak Kapur (Albany SU, USA) Dave Musser (RPI, USA) Tobias Nipkow (Univ. of Cambridge, UK) Paolo Prinetto (Politechnico di Torino, Italy) Clive Pygott (RSRE, UK) David Shepherd (Inmos, UK) Joseph Sifakis (IMAG, France)

IMPORTANT DATES

The important dates are as follows:

30 September 1991 :

Final deadline for the submission of papers.

28 February 1992 :

Date for notification of acceptance or rejection.

30 April 1992 :

Final camera-ready copy due.

22-24 June 1992 :

```
Conference at Nijmegen.
```

SUBMITTING A PAPER

Four copies of a complete paper (in English) should be sent to the Programme Chair at the address given below to arrive no later than 30 September 1991. Papers must not exceed 6000 words in length, with full-page figures counted as 300 words. Each paper should include a short abstract and a list of keywords for subject classification. All papers will be refereed and the final choice will be made by the programme committee on the grounds of relevance, significance, originality, correctness and clarity. Submitted papers must not be published or under consideration for publication elsewhere in the same or similar form. Authors of accepted papers will be sent LaTeX style files to aid in the production of camera-ready copy.

PROPOSALS FOR TUTORIALS

Proposals are solicited for tutorial presentations on relevant theorem proving technology or tools. The intention is that a tutorial will provide an overview of the basic ideas behind a theorem proving tool, rather than detailed instruction in how to use it. Tutorials should include an assessment of strengths and weaknesses of a tool and should concentrate on general issues such as security, robustness, the degree of interaction required, the user interface, and the mathematical skill required of the user.

Proposals for tutorials should not exceed 1000 words in length and should give a clear indication of the topic and structure of the presentation. Also welcome are proposals for informal demonstrations of working systems. Proposals for both tutorials and demonstrations should be sent to the Tutorials Chair at the address given below to arrive no later than 30 September 1991.

ADDRESSES FOR CORRESPONDENCE

Papers and all general correspondence should, in the first instance, be sent to the Programme Chair at the following address:

Victoria Stavridou, TPCD Programme Chair, Department of Computer Science, RHBNC , University of London, Egham Hill, Egham, Surrey, TW20 0EX, United Kingdom. Tel: (+44) 865 273808 (until 30/9/91) Tel: (+44) 784 443429/3421 (after 30/9/91) Fax: (+44) 865 273839/784 437520 Email: victoria@cs.rhbnc.ac.uk

Proposals for tutorials and demonstrations should be sent to the Tutorials Chair:

Tom Melham, TPCD Tutorials Chair, Computer Laboratory, University of Cambridge, New Museums Site, Pembroke Street, Cambridge, CB2 3QG, United Kingdom. Email: tfm@cl.cam.ac.uk

All correspondence should include a return postal address and, if possible, an electronic mail address.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Pete Mellor <pm@cs.city.ac.uk> Tue, 29 Jan 91 22:00:48 PST

Tube train's open doors beat fail-safe (By-line: Dick Murray) London Evening Standard, Thursday, 24 January, 1991

A tube train travelled four stops with a set of double doors open after its "fail-safe" system broke down, it was revealed today. The driver was not aware of what had happened until alerted by an off-duty Tube manager who was travelling on the Circle-line tube at the time.

London Underground has always described such an incident as "the one which could never happen", and now seriously concerned engineers are worried that a similar fault might occur on other trains.

The train has had a detailed examination and a full inquiry began today. Luckily, the incident happened at one of the quietest times of the week, early on a Saturday morning, but drivers are now worried about the consequences of a similar incident taking place on a crowded rush-hour train.

London Underground says the driver of the train, which travelled between Aldgate and Farringdon [the stop at which I get off! - PM], was not at fault. A light in the cab's control panel tells a driver when all doors are closed. If a door does not close, the "fail-safe" system should come into operation and prevent it from moving off. But in this case - the train was driver-only with no guard [Sorry to say "I told you so!", but see my previous mailing! - PM] it seems the fault may have affected the panel light operation and the automatic "fail-safe" system. One driver said: "He got the light that that everything was OK. He acted by the book."

An Underground spokesman confirmed the incident took place on Saturday, 12 January, and said: "The 6.18am from Aldgate was taken out of service at Farringdon after a report from a supervisor on the train. A set of doors remained open but it appears the driver was not aware of this. It would appear to have been a train malfunction."

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

IRS overbills for \$1B interest

"Peter G. Neumann" <neumann@csl.sri.com> Wed, 30 Jan 1991 10:15:21 PST

Having ruled that Dickie Ann Conn of San Jose CA owed \$67,714 in back taxes, the IRS billed her for more than \$1 billion (including penalties). (The ruling was based on the precedent of a recent court case, and stemmed from charitable deductions to the Church of Scientology that Conn had claimed over six years.) When she called the IRS to object, she was told by a clerk that her only recourse was to sue the government. Yesterday the IRS admitted that they had found a mistake in the interest calculations, and said they will correct it. [Source: San Francisco Chronicle, 30 Jan 91, p.4] (Conn is a computer consultant and part owner of Connsult Inc. She is probably used to jokes about Conn Jobs, but in this case it sounded as if the IRS was trying to be Conniverous.)

Ke: Patriots (Wegeng, <u>RISKS-10.83</u>)

Dave Parnas <parnas@qucis.queensu.ca> Tue, 29 Jan 91 17:35:20 EST Don Wegeng writes that sensors that were developed as part of the SDI research program, and first tested about six months ago, are now deployed on the thousands of Patriots in the field. This is so inconsistent with my experience with DoD deployment that I would not believe it unless the source was willing to be identified. There is a long road between first tests and deployment and it is not usually travelled in six months.

One should also note that this would mean that SDI money was used to enhance the Patriot, not that SDI software technology was used to enhance the Patriot.

Dave Parnas

Kisks of automatic flight (flying at low level) (<u>RISKS-10.83</u>)

Brinton Cooper <abc@BRL.MIL> Wed, 30 Jan 91 9:39:30 EST

Olivier M.J. Crepin-Leblond <MEEB37@vaxa.cc.imperial.ac.uk> reports on the risks of automatic flight (flying at low level) incurred by fighter pilots:

Perhaps the U.S. Air Force should consider abandoning HUMAN pilots for very low altitude flights of this type. As the proposal often begins,

"Research is required ... "

Automated brokerage service

Kent M Pitman <MP@STONY-BROOK.SCRC.Symbolics.COM> Thu, 20 Dec 1990 15:38 EST [recently resent, never previously received]

My company's stock recently did a one-for-ten reverse split and I wanted to follow the changes in its price. I figured I might as well use the Charles Schwab 24-hour 800 number with `automated telebroker,' so I could just punch in the stock symbol and get info automatically.

I did this a few times at intervals after the split, and it kept telling me that it was bid at 2-1/4, and asking 2-7/8. Eventually I became suspicious. Finally I heard a different price from someone and decided to call Schwab and find out the straight story.

The guy tried to call up the price of SMBX on his computer and said it wasn't there. I assured him it had worked when I tried. Then he said, ``oh, it's trading under a new symbol--SMBXD. It's at--'' and I forget exactly what price he quoted but it was in the low 1's.

So my stock [fortunately not major dollars] had lots half its value and they hadn't kept me aware. Great. [I wondered if there was any recourse, but somehow doubt it.] The guy agreed it was a problem that should be fixed and promised to notify the appropriate people.

Pretty clearly the bug was [and perhaps still is] the presence of an open

record for an account that was `renamed' when the reverse split occurred.

I called a couple days later to see if it had been fixed. Nope. At first the attendant denied that you could call up such a record, and then said ``oh, are you using that telebroker service?'' What did he think I was using? The first thing it says when I call up is to press `1' for the service if I'm using a touch-tone phone. Then when I explained the story about how I'd asked that it be fixed, he said (as if this explained off the problem) ``well, that's an automated service.'' He went on to add something to the effect of ``If you really cared, you should have followed it more closely and noticed the problem sooner yourself.''

>From a corporate point of view, I thought he put forward a phenomenally bad image for his company and I will pursue my that gripe via the company's customer relations department. But from a pragmatic technological standpoint, he was probably right. Being in the computer business, I should probably have known enough to understand that even an automated system like that still relies on lots of human care and feeding, and is likely to have lots of problems. Still, I wonder how many non-computer people understand that risk.

The other thing that bugged me in talking to him was the fact that I tried to explain why it was a bug that when I asked for the dead account, it echoed back ``Symbolics Incorporated'' when all I'd punched in was its code, 73612292 [their telephone keypad code for "SMBX"]. But even now, when I punch in the right symbol, 7361229231 ["SMBXD"], it echos back "ess em bee ex dee" and doesn't give me tons of confidence that I'm even asking about the right thing. He didn't seem to see why that was a problem. I tried explaining several different ways why it was important for the system to echo back something meaningful after I pressed a bunch of digits so I could know I'd pressed the right ones, and he couldn't seem to grasp why I felt that hearing the right name after punching the wrong digits contributed to my feeling of having been deceived, or why it bothered me that even now if you pressed the right digits you heard something that was not the name of the company.

There should be a place in the world where you can send bug reports about companies whose facilities for accepting bug reports are broken. In the long run, the free market may attend to these things, but in the short run that's not much of an answer.

Ke: Broadcast local area networks are a'comin (Tom.Lane, <u>RISKS-10.83</u>)

Brinton Cooper <abc@BRL.MIL> Wed, 30 Jan 91 9:44:24 EST

Tom.Lane@G.GP.CS.CMU.EDU reports on the filing by Apple computer for allocation of radio bandwidth to implement wireless local radio networks. He correctly observes

>The risks should be pretty obvious to readers of this digest. Somebody in
>the next building could eavesdrop on your traffic, or actively connect into
>your net, with NO special hardware. I sure hope Apple is at least planning
>to encrypt the packets... (But if they are going to support 10Mb/sec data rates, the

>encryption would have to be fairly weak, methinks.) ...

Beyond this, the risk for spectral chaos seems to be quite high. Imagine the RFI (radio frequency interference) implications of a central city full of wireless ethernets(tm?) attempting to coexist with cellular phone, radio paging systems, public safety radio, business use of dispatch radio, amateur radio repeaters, etc. Pulsed signals 10 Mb/s may well wreak havoc in many such receivers.

_Brint

Marcadcast local area networks are a'comin

P.J. Karafiol <karafiol@husc8.harvard.edu> Wed, 30 Jan 91 09:52:44 -0500

This summer I saw ads for a similar product: Appletalk LANS created by a system of infrared transmitters and receivers. The idea was that each desk would have a doodad that would bounce the signals off the ceiling; the system was designed for a cubicle-type environment where offices were reconfigured frequently. It was about \$500/connection. This seems more reasonable than the radio LAN because we are talking about a true line-of-sight kind of communication; besides, the beams were only sufficiently intense for about 150'. To intercept this LAN would require a listening (watching?) post *outside*the*window* of the offices in question. The obvious defense would be to locate on the 56th floor

. . .

== pj karafiol

Ke: Re: Electronic cash completely replacing cash (Lamb, <u>RISKS-10.82</u>)

Bob Stratton <dsc3rjs@nmdsc20.nmdsc.nnmc.navy.mil> Tue, 29 Jan 91 15:51:10 EST

> ...There's a prophecy in Revelations about "the mark of the Beast" without> which one could neither buy or sell. ...

As I understand it, the world's largest EFT (electronic funds transfer) computer, which I believe to be in Switzerland, is affectionately nicknamed "The Beast", and more than one religious group has capitalized on this fact in its literature. (I've seen some of it, but it was a while ago...)

Bob Stratton, Stratton Systems Design, strat@ai.mit.edu +1 703 823 MIND

Ke: Electronic cash completely replacing cash (`witt', <u>RISKS-10.81</u>)

Rick Smith <smith@SCTC.COM> Tue, 29 Jan 91 17:35:19 CST

As a "cash resistant" individual, I enjoyed reading the proposals to "eliminate cash." Personally, I usually carry only enough cash to pay for lunch for the

week, and use credit cards for everything else.

But I don't think the "Americard" proposal would work. Not in America. The author's recommendations require the assignment of a unique number that gets copied and used in virtually every transaction. This sounds like a clone of the Social Security Number, and I think the current trend in restricting use of SSNs bodes ill for the implementation of similar numbers. It is also not clear whether the author expects that private credit card organizations will be put out of business for this government boondoggle, but it seems to be implied.

Most people know that their credit card numbers and Social Security numbers are sensitive information. You don't give your credit card number to just anyone. Right now, credit card numbers are used by a fairly restricted set of organizations. The banks who process credit card purchases for stores are very careful about the stores they work with. The bank and store are very, very interested in the security of these transactions. The store doesn't want any improper credits and the bank doesn't want any improper sales. Credit slips go into a special pile that unauthorized people can't go looking through. But if every Tom, Dick, or Harriet can plug in their Americard reader and post "payments" from other people, how soon will it be before someone builds the new generation "blue box" that steals money electronically?

Muggers and bu[r]glars would be out of business: no one would
 be carrying cash and stolen property would be difficult to sell
 because there would be records of all transactions....

Burglary begins at home. Why hit the streets if you can steal it all with a little box of electronics?

> Think about it. Drug deals, muggings, corruption, businesses
 > concealing their income - they all require cash and secrecy. A
 > monetary system bases solely on electronic currency would leave a
 > trail that would cripple such enterprises.

And people will establish electronic laundries to undo all of this. Transactions will identify buyer and seller, and probably include some transaction-specific code agreed on by the buyer and seller. For example, if I'm paying my phone bill I use code 1234506 and if I'm paying for overpriced repair services I use code 9876765, both paid to the phone company. Or, if I'm trying to launder a transaction, I funnel it through some bizarre set of recepients with a peculiar set of transaction codes. The recipients have to be in on it, of course, so a good laundry would probably be a regional fast food chain, for example. In order to trace laundry transactions you'd have to reconstruct numerous "small" transactions and follow them through accounts that would be gone when investigators went looking for them.

The only way to prevent such laundering would be to pass laws, laws, and more laws, trying to stay ahead of potential data paths. Most of the laws would be unenforceable without a platoon of data police. You'd bind up business with so many transaction regulations that the economy would grind to a halt. And we'd get a centralized economy that even Josef Stalin would envy. As it is, a variety of small businesses have special treatment under currency reporting regulations. That keeps them from going out of business due to excessive regulatory paperwork. >... The benefits would be tremendous. Individuals and businesses
 >would no longer be able to conceal income. All transactions would be
 >recorded in a computerized bank file and would be easy for the I.R.S.
 >to check....

This is a benefit? I don't think the proposer has any idea how massive such a file would be. It took the IRS years to set up a fairly mundane procedure to cross check income reports against individual tax returns. That handled millions of transactions per year. The other database would be millions per day, if not per hour. People could conceal income by just refusing to report it twice. Data like that can only be used after they filter it. The only things they'll find are things they look for. You bypass such things by hiding the "bad" transaction behind a set of "good" ones. And it's just a case of staying one step ahead of their filtering program, which can't look for everything. After all, it's only a computer.

Finally, some economic considerations:

In place of paper money, we would receive new cards - let's
 call them Americards - each bio-mechanically impregnated with the
 owner's hand and retina prints to insure virtually foolproof
 identification. ...

>At lunchtime, you would go to your favorite [restaurant] - or the local >hot dog stand - and instead of paying cash, you'd use your Americard.

This is the technological battering ram hitting the proverbial fly. Each hot dog stand needs a high reliability, secure, bidirectional link to the international electronic funds financial network (typical hotdog stands don't even have telephones, after all). This link is connected to a device that does pattern recognition on fingerprints or retinas, and reads some data off of a card. Finally we find it attached to a numeric keypad. And it's probably as easy to use as a helicopter. As a kid I remember predictions of the "mass market personal airplane." It never happened. Some technological systems are too costly. I expect the bio-identification and the security problems will keep the costs of "Americard" very high indefinitely.

In any case, how do you know you can trust a cheesy vending machine at some gas station to charge you a quarter and not \$25.00 ?? We already have that problem with pay phones.

Rick Smith, SCTC, Arden Hills, Minnesota

Re: <u>RISKS DIGEST 10.82</u>

Stephen Perelgut perelgut@turing.toronto.edu>
Tue, 29 Jan 91 21:59:13 EST

More cash-card questions (from an infrequent reader). What happens to people travelling from outside the U.S. Do we stop at immigration and get an Americard? Is it a credit card, debit card, ??? What about Americans travelling outside the country? Surely they would use the
appropriate currency. I'd guess that Canadian \$'s would become the coinage of the underground marketplace thereby artificially inflating the value of \$CDN thereby destroying one of our economic underpinnings.

✓ Electronic cash completely replacing cash

Art Medlar <art@big-ben.UUCP> Tue, 29 Jan 91 20:27:09 PST

If all the people who do business in cash were forced to report
 their incomes accurately - if the under-ground economy were forced to the
 surface - the Government could collect an additional \$100 billion a year
 for the nation[a]I treasury - without raising taxes. States and cities, many
 in serious financial trouble, would also benefit from collecting
 previously unpaid income and sales taxes.

Though not all would agree that this is a RISK of the technology (as opposed to a benefit), certainly one potential outcome of Mr. Wachsman's scheme would be the enhancement and strengthening of the very underground economy he seeks to destroy; and consequentially the elimination of even more tax income from the national treasury. An active, established barter system, and a thriving black market economy based on the easily convertible currency of some foreign country, would tend to destabilize and decentralize the control of the monetary system.

But it's in the subtext of Mr. Wachsman's loopy proposal that the real RISK lies. I've heard that there's a delightful Yiddish word, "farpotchket" I think, which means not simply broken, but broken because somebody tried to fix it. The danger of the haphazard application of computer technology to situations that are really getting along just fine in the first place should be apparent to all.

--art

Cashless society

C-News <news@eng.umd.edu> Wed, 30 Jan 91 09:37:22 -0500

The risks of a cashless economy are charmingly illustrated in the fiction of Frederik Pohl. I especially recommend The Space Merchants by Pohl and C. M. Kornbluth.

[The c-news are tensed these days? Who are you?]

Ke: Electronic Cash

Unix Guru-in-Training <elr%trintex@uunet.UU.NET> Wed, 30 Jan 91 08:59:54 EST

For an excellent treatment of how easily an electronic cash system can be

abused by the government in power, check out "The Handmaid's Tale" by Margaret Atwood. The theme is a Christian Fundamentalist takeover of the US Government. In one scene, the new government in power decides that women shouldn't be allowed to handle money (hmm... sounds like Saudia Arabia, doesn't it). Everyone in the country was already using an "Electrobank" card system, and women's account numbers ended in an even numbered digit. One day everyone wakes up and women's cash cards don't work anymore. All their balances were switched to their husband's, father's or other patriarchal figure (such as the government itself).

The simplicity of Atwood's scenario and its nearness to our current reality is chilling. (This applies to most of the scenarios in the book.) I was especially struck by this section, perhaps because in spite of the fact that I work with computer networks every day and consider myself well informed on these threats to our civil liberties, 1984 just never seemed so close as when I read this novel.

Ed Ravin, Prodigy Services Company, White Plains, NY 10601 philabs!trintex!elr +1-914-993-4737

Comment on all electronic currency

Leslie DeGroff <EGROFF@GENIE.INTELLICORP.COM> Tue, 29 Jan 91 14:02:53 PST

Being a day behind on reading risks many of my comments have been made by others but I would like to make two additions to the commentary, The "Underground" economy is a vigorous part of the system and in many places and times when the official currency of a country is at risk, either by price and bank controls or by simply not being worth much you find that the most valued street money is some other countries currency. For example in many parts of asia or eastern europe a greatly desired street currency is US dollars... which are generally not easily exchanged locally for official goods or currency. The coupling of the official currency and the subeconomy by cash is not typical or required for it to work. Note also the current Soviet attempt to withdraw large bills from circulation... partly to try and weaken the subeconomy.

A second point that I think is critical is that such a scheme has many attractions to banks and government officials and in a severe financial crisis might be sold to the American public (or at least to the elected officials) Among it's attractions besides better control of taxation; more precision in economic statistics, ability to quickly deflate/inflate currency especially in regards to foreign exchanges (out of one currency into another). Such a system is an attractive trap and one that one can slip slowly into..

today (credit and debit cards (more than one per American) legally mandated reporting of large cash transactions S&L and bank problems and discussion about limits on government backed deposit insurance) tomorrow (tax's need to be paided by transaction card with valid ID

Social Security cards that are magnetic media

http://catless.ncl.ac.uk/Risks/10.84.html[2011-06-11 08:17:41]





"Jay Elinsky" <LINSKY@YKTVMZ.BITNET> Thu, 31 Jan 91 08:58:53 EST

On "Neighbors" page of Woman's Day, 5 February 1991: A husband who finds it difficult to say "I Love You" programmed his wife's software on their personal computer to flash "I LOVE YOU" on the screen when she exits the program.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

[This is known as putting all your exits in one pass-kit. But what, you might ask, is the RISK that makes this story relevant? The Trojan horsing around? The risk of botching her software? The opportunities for subliminal advertising?

Well, when Weekly World News prints this story, it will describe it as intelligent workstation software that gets jealous because it detected the amorous intent of the husband and then automagically changed the message to

"YOUR HUSBAND IS CHEATING ON YOU." or "YOUR HUSBAND IS TRYING TO BUG YOUR SOFTWARE." PGN]

Ke: Auto Pilot Problems

"DAVID B. HORVATH, CDP 8*747/215-354-2468" <ORVATH_DB@scov19.dnet.ge.com> Wed, 30 Jan 91 15:35:58 EST

During the Vietnam war (conflict?), the F-111 was sent into combat. There are three modes to the terrain following equipment - soft, medium, and hard. These modes describe how hard the computer climbs or dives the aircraft - the number of G's exerted on the crew.

Several planes were lost shortly after deployment. Another crew reported that when the hard mode was used, there were times that the crew was helpless - the computer performed 5 G climbs and dives over some of the high hilly terrain in vietnam. The plane would climb HARD and dive HARD, climb and dive, etc.; due to the G-forces, the crew was not able to control the plane, making it a good target for the enemy.

Being air-sick is nothing compared with being shot down because you can't take the airplane's controls out of automatic mode.

- David Horvath

[Opinions are mine only; I found this information in something I read. References available on request.]

Ke: Risks of automatic flight (Crepin-Leblond translation, <u>RISKS-10.83</u>)

Gordon D. Wishon <gwishon@blackbird.afit.af.mil> 31 Jan 91 22:03:36 GMT

> This is so serious that when some pilots arrived at the target site, they had
 >lost all faculties of analysis, and as a result the U.S. Air Force has decided
 >to abandon at least partially the concept of automated piloting for very low
 >altitude flights. "

Ahem... I hope someone tells the crewmembers of USAF F-111's, RAF Tornados, and any allied LANTIRN-equipped aircraft (among others).

It's ludicrous to believe that any airman would allow his pink flesh to be routinely thrown at the ground without some control (or at least a cross check) of the system. I would suspect that's the real reason to "abandon" the concept. Don't forget, in the USAF at least, airmen make the decisions on what technology to pursue. As for airsickness, some people are susceptible, others are not. Those who are, are mostly weeded out during the qualification process.

By the way, the article should have specified "...the concept of _manned_ automated piloting...." The concept of unmanned automated piloting is alive and well (vis. Tomohawk cruise missile).

Gordon D. Wishon, Air Force Institute of Technology

Re: Patriots (<u>RISKS-10.84</u>)

Alex Bangs <abg@mars.EPM.ORNL.GOV> Wed, 30 Jan 91 15:46:02 EST

Note that according to press reports, the JSTARS tracking aircraft is being used in the Kuwaiti theater. This aircraft is only a prototype. I remember hearing early on that JSTARS would _not_ be used because they didn't want to risk it, but apparently they have decided otherwise. Or the press could be wrong.

Alex Bangs, ORNL

🗡 Patriots

Jerry Leichter <leichter@lrw.com> Thu, 31 Jan 91 00:16:38 EDT

The debate about what the apparent effectiveness of the Patriots demonstrates itself demonstrates the unfortunate way in which too much debate on various important issues is carried on.

1. The Patriot was intended to be a close-in defender of important military sites. It was apparently never intended to be used to defend cities.

When you are protecting a relatively small, fairly "hard", military site, knocking an incoming warhead off target by even a fairly small amount is an excellent defense. Obviously this is NOT the case when you are defending a spread out, fairly "soft" target like a city.

2. "If the warhead had chemical agents, blowing it up with a Patriot just makes things worse." Simple logic tells you that this is unlikely to be true. There is an optimal height at which to release poison gas: Too near the ground and it doesn't spread out enough, too high and it dissipates before having an effect. The designer of the warhead will try to hit the optimum. Unless he does a really bad job of it, AND you are very unlucky, you can at worst leave things unchanged by hitting the warhead.

The arguments in (1) and (2) are typical of one class of responses by those who have an emotional attachment to the position that sophisticated weapons don't work: When the systems SEEM to work, that's only an illusion - they don't REALLY work after all. (I'd be interested to know what those who make these arguments think the Israelis have in mind in deploying and using Patriots.)

The arguments of those who have an attachment to these weapons are pretty much the same, if turned around: See, they work so they are effective. The evidence - so far as we can tell through the noise of battle combined with censorship - is that these weapons really DO work, in the sense that they do pretty much what their builders claimed. What is by no means clear is that they are as effective at actually doing something USEFUL, as has also been claimed.

A more subtle anti-smart-weapon argument takes the form: "Well, yes, these things work, but we always knew they would - it's those OTHER things that don't work." The difficulty with such a claim is that anyone can make it after the fact. Certain people - David Parnas is certainly one, as he has written about many of these issues - can legitimately and honestly say that they have never said, say, that close-in defenses can't work, they've only argued against some more grandiose schemes. However, my own experience has been that most critics had very general complaints about these systems. "They won't work in the heat of battle." "The sand will destroy them." "RFI among all the planes in the sky will make them all do crazy things." And so on. In effect, these people made a prediction: When used in battle, these devices would not perform as well as simpler weapons. As far as we can tell at this point, that prediction was just plain wrong.

I must admit that I made such predictions myself. Having seen the way large complex systems fail, especially having seen how getting the last 10% can destroy the 90% you already have, I always read the criticisms with great sympathy. If you had asked me a couple of months ago whether one could expect to hit rockets coming essentially straight down at Mach 4, in the middle of a desert, night after night, with all sorts of other clutter in the sky, I would have said "no". (It appears that Parnas knew better.)

A final argument, seen on both sides, is essentially one of extrapolation: Sure, you can hit SCUDs, but what about the next weapon? Sure, a Stealth fighter can hide from standard radar, but what about two-point radar? To which the only answer is: Weapons are always changing. They have been since the beginning of time, and they always will be. The best you can do is match what the other guy has now, or will likely have in the near future. In the long run, both your system and the other guy's will be obsolete; it's a neverending process. At the moment, the evidence is that the smart weapons CAN be built and used, and can best "not so smart" weapons. Things could change.

The same argument from the other side is: We can build a Patriot, so we can build an SDI. Well, maybe - but that's a very big leap. On the other hand, the claim "We can build a Patriot, so we can build an ABM system that will keep us safe from attack by any small power (i.e., an attack with no more than a few hundred warheads)" is now at least reasonably arguable.

It's been said that the first victim of war is the truth. There are plenty

of issues here - political, social, technological, military - that need to be examined with some degree of rational thought. Sloganeering doesn't help. Refusing to look at the evidence doesn't help. Refusing to change one's mind no matter WHAT happens doesn't help.

-- Jerry

Patriot missiles provide no evidence for SDI

Martyn Thomas <mct@praxis.co.uk> Thu, 31 Jan 91 14:03:52 BST

One powerful argument against SDI is that you need confidence that the system will work effectively the first time it is used against a full attack. The Patriot missiles, even if they were 100% effective against SCUDs, can provide no basis on which we can be confident that a different system, deployed against different targets, would be successful.

In general, we may be able to *achieve* very high success rates with complex systems, but this is a very different thing from being able to *predict* a high success rate with any convincing evidence. When we certify a new safety-critical system for use, we predict that the failure rate will be acceptable; evidence that past systems have achieved acceptable error-rates is almost useless for justifying such a prediction, unless the new system is a very well-controlled evolution of the earlier system. This is extremely rare.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. +44-225-444700.

Ke: Patriot Missile (Parnas)

<henry@zoo.toronto.edu> Thu, 31 Jan 91 11:54:47 EST

I should preface this by saying that I agree with Dave Parnas's most basic point: recent Patriot successes say little about effectiveness of more ambitious antimissile defences. However, some of his arguments are weak...

>...The Patriot missile itself is launched on a path that will
>intercept the path of the incoming missile ...
>and has a very simple homing system that is effective when (and if) it
>gets near its target. Were the target missile to change course drastically
>after launch, the Patriot missile would end up somewhere else...

I believe this is erroneous. Patriot is guided, under control of the launch system, all the way up. It's not a question of firing it on a predetermined trajectory in hopes that it will get close enough to home. Even Patriot's homing is actually controlled by the ground computers; the missile itself has no brains to speak of, just a receiver system that picks up radar reflections off the target and relays them to the ground for assessment. In principle, a drastic course change by the target can be matched by a similar change by the Patriot. How well this actually works is an open question, since it hasn't been tried in combat. (The recent incident of an accidental launch against aircraft is silly as a test case, since the Patriot system reportedly was in antimissile mode and thus probably wasn't expecting evasive action.)

It occurred to me a little while ago, in fact, that we may never know how well Patriot would work against aircraft. Aircraft can be shot down by lots of systems, e.g., other aircraft, while Patriot is the only operational antimissile system. I'd expect that the Patriot batteries in the Gulf have firm orders to ignore aircraft, and it would take a really drastic change in the situation to get those orders changed.

>... The development and manufacture tooling stage of the Patriot
>was completed in 1980... The SDI program was
>not announced until 1983. There was no SDI software technology to be applied
>to Patriot...

While the original development of Patriot was completed about a decade ago, much of the antimissile capability was in the form of retrofits. According to Flight International, full production of Patriots with the current antimissile capability started in 1989. So there was some opportunity for application of SDI software technology, although I do not know whether that actually happened.

>... Terminal defense systems can have an operator who makes>decisions that would have had to be automated in the space-based system.

I've never understood why it is fundamentally impossible to put "man in the loop" for space-based systems. I'd be interested in seeing this explained. There is clearly a serious shortage of time for decision-making, but the same is true of terminal defence against tactical missiles -- which have much shorter flight times than ICBMs -- and short-notice decision-making in combat is both possible and practical, as any fighter pilot can testify.

>... The SCUD was first deployed about 1965 - Patriot about 19 years later.
 >All RISKS readers should think about the advances that we have seen in 19
 >years. It should come as no surprise that the Patriot can sometimes destroy
 >missiles that were deployed when its development began...

As far as I am aware, it should still be capable of destroying most missiles that were deployed yesterday. Maneuvering warheads remain extremely rare and rather limited, and most other forms of countermeasures don't work in the terminal phase.

Henry Spencer at U of Toronto Zoology utzoo!henry

Patriot's defense (Johnson, <u>RISKS-10.83</u>)

Frank Ritter <fr07+@ANDREW.CMU.EDU> Thu, 31 Jan 91 03:16:54 -0500 (EST)

Some notes on the Patriot system:

You can "program" by designating areas where all planes are safe, or a plane should be assumed a bogey. The programming going on now is probably on this level, where they are trying to create areas not to shoot at what's in them. There are things that could be used, but I don't think anything provided directly or played with in the past.

I know that a good way to avoid Patriot missiles is to drop below their radar height. I would also assume that if I had accidently shot at a friendly, I would give them a call and turn off my radar. Even if neither of these occured, our pilots are keenly aware and concerned about the Patriot system and how to avoid it (and indeed all air defense, ours and theirs). And there are other ways to beat the Patriot, such as being in a "safe zone" that change daily, which friendlies, and only friendlies, would know. I don't think what we've seen tells me a lot. SCUDs are a lot different than planes, while they travel straight, they travel darn fast for a plane. Our planes should be able to not get hit even if shot at, particularly if there are no other planes or AAA.

The real power of the Patriot appears to be the ability to deal with a large number of planes, some targets, some not. If these friendlies came back without their transponders on, in the wrong direction and altitude, the right mistake was to shoot at them. Until you know this information, it's hard to judge what was going on.

Frank Ritter@cs.cmu.edu ritter@psy.cmu.edu fr07@andrew.cmu.edu

Nike Hercules Site (Re: Patriots, Wright, <u>RISKS-10.83</u>)

"DAVID B. HORVATH, CDP 8*747/215-354-2468" <ORVATH_DB@scov19.dnet.ge.com> Wed, 30 Jan 91 15:35:31 EST

> Some years back I was stationed with HHB 45th Arty (AD) a Nike Hercules unit > [...]

> the reply was "Well son what would you rather have: ## kilotons over > Evanston, or 10 to 50 megatons over the loop ?" [... Ed Wright]

I live in suburban Philadelphia (Pennsylvania, USA), a few miles from where I live is the remains of a Nike Hercules unit. I believe the intent was to loose Broomall or Cherry Hill (New Jersey) to save Philadelphia and other suburbs. I can see a conversation like the one described above actually happening!

- David Horvath

Ke: Broadcast local area networks are a'comin

&uss_Housley.McLean_CSD@xerox.com> Wed, 30 Jan 1991 11:06:04 PST

In <u>RISKS 10.83</u>, Tom Lane quotes an article from the New York Times stating that Apple is installing (or at least reserving the radio frequencies for) a wireless 10 Mbit/sec LAN. Tom observes that such a broadcast LAN requires protection. I agree.

Wireless LANs are being standardized by the IEEE and IEEE 802.11 was recently

formed for just this task. The people working on this standard also agree that sensitive data must be protected on such a LAN. IEEE 802.10 (Standard for Interoperable LAN Security) is developing standards for just this purpose. (Of course, it would be up to each company to decide whether all its data is sensitive.)

Tom Lane also says, "(But if they are going to support 10Mb/sec data rates, the encryption would have to be fairly weak, methinks.)" On this, Mr. Lane and I disagree! 10 Mbit/sec is the data rate of the "backbone." If encryption is placed at each wireless LAN station, the encryptors can run at a significantly lower data rate. The station cipher device only needs to decrypt those frames which are addressed to that station. Of course, this includes broadcast frames, appropriate multicast frames, and frames addressed to that particular station.

In the IEEE 802.3 (Ethernet) world, there are encryption devices that work just this way. I will refrain from turning this into an advertisement for such products, but they are available with the DES algorithm and with NSA "proprietary" algorithms.

Russ Housley

broadcast LAN's

frank letts <letts@ficc.ferranti.com> Wed Jan 30 22:45:06 1991

Reading the notices about the approach of broadcast LAN's reminded me of a semihumorous incident that happened about 2 years while I was doing some consulting for a "local" oil company. We were preparing a SCADA system for Oilpatch, Texas and had the entire thing staged on the 17th floor of a TALL building in downtown Houston. (That ought to narrow the oil company down to about 20 or so.) All of the remote telemetry units were communicating with the master station computer via low power Johnson radios, and I had made sure that we had dummy loads on all of the antennae so as to cut down the range of the transmissions. This screwed up SWR's and about everything else, but we could adjust the transceivers and get decent communications - most of the time. Sporadically, we would get bursts of errors for seemingly no reason, and then good comm again for a while. I hooked up data analysers, etc, and could see the junk that was being injected on the frequency, but couldn't identify it as any of the other equipment that we had operating in the area.

I remembered an old microwave hand showing me how you could kluge in a telephone handset on a circuit and listen to the "noise", often identifying it with ease when all of the sophisticated techniques had failed. Out of desperation, I rigged up a speaker at the master station and listened to the buzzings of the remotes answering the master. Much to my surprise, I heard some poor fella in a delivery truck complain about "there's that doggone buzzing sound again" to his dispatcher at the same time that our comm efficiency dropped to zero!

I felt sorry for him, but I didn't have enough radios laying around to set up with another frequency, so we just kept testing with the occasional comm burps

until we shipped the system. I did leave the speaker hooked up, though. It was kinda fun listening to all of those guys swear at the strange interference that they were getting.

Frank Letts, Ferranti International Controls Corp., Sugar Land, Texas (713)274-5509

[Sounds like the old joke whose punchline is "Hey Martha, it's that guy with the damn whistle again."

Ke: Risks of radio-based LAN's (Lane, <u>RISKS-10.83</u>)

Rich Rosenbaum 30-Jan-1991 1029 <rosenbaum@took.enet.dec.com> Wed, 30 Jan 91 16:31:24 PST

In <u>RISKS-10.83</u>, Tom Lane points out the security risks of wireless (radio-based) LAN technology. Actually, wireless LAN's have the potential to be _more_ secure than traditional "wired" LAN's.

One currently available wireless LAN product uses spread spectrum communications. (It is interesting to note that, for the radio frequencies used by this product, the FCC mandates use of spread spectrum).

While I am not an expert on spread spectrum communications, my understanding of the technique suggests that it offers both increased protection against eavesdropping as well as resistance to jamming, when compared to traditional radio broadcast techniques.

Rich Rosenbaum

Marcadcast local area networks are a' comin

Ian Clements <ian@lassen.wpd.sgi.com> Wed, 30 Jan 91 17:29:59 PST

One other possible risk is to those with pacemakers or other electronic medical devices (such as implanted pumps or heart monitoring devices).

--ian Ian Clem

lan Clements ian@sgi.com 415/962-3410



Search RISKS using swish-e

Report problems with the web pages to the maintainer