

## Re: "Miracle" computer-controlled piano teaching (Scott E. Preece, Ed Nilges)

## Issue 04 (20 January 1992)

- Russian Computer Productivity in AScent in de Scent Exposure
- Gulf war virus? [2] (Phil R. Karn)
- Re: PC virus infects UNIX system (A. Padgett Peterson)
- Ohio justices fight over computer snooping (Dave Harding)
- <u>Rumor: No 1992 for AT&T? (Thomson Kuhn)</u>
- Another ATM Risk story (Josh Quittner)
- Words for theft of passwords (Mark R Cornwell)

## Issue 05 (22 January 1992)

- Another A-320 crash in France (Paul)
- California Judge recommends NO on CALLER ID (PGN)
- Re: Gulf war virus? (Andrew Klossner)
- Chicken Little and the Computer (A. Padgett Peterson)
- <u>CPAs leary of electronic filing (Paul Schmidt)</u>
- Re: AT&T machines and dates (Chris Traynor, Daniel J Yurman)
- <u>A Tale of Risk Avoidance (Kai-Mikael J\d\d-Aro)</u>
- A little knowledge can lead to understanding ... (Armando P. Stettner)
- <u>Risk of computer-generated overhead foils (Jonathan Bowen)</u>
- MacNeil/Lehrer Report on Phone System Risks (Randall C Gellens)
- Re: Automated bill collectors, privacy, ... (Marc Shannon)
- Re: Ohio justices fight over computer snooping (Bob Frankston)
- IEEE Software Safety (Tony Zawilski)
- IEEE Oakland Security and Privacy Symposium Preliminary Program (John McLean).
- Issue 06 (24 January 1992)
  - A320 (Peter Mellor, T.C.Bennett, Ken Tindell)
  - Computerized Chauvinism (Brian Randell)
  - "Desert Storm" viral myths (Rob Slade)
  - "Designed-in Hardware Viruses" in the movies: "GOG" (Lauren Weinstein)
  - Sharing Idle Time with Linda (David C Lawrence)
  - Software Safety Correction (Tony Zawilski)
  - Re: Ohio justices fight over computer snooping (Christopher Stacy)
- Issue 07 (25 January 1992)
  - Re: A320 crash (Philippe Colbach, Robert Dorsett, Kraig Meyer, Eric Florack)
  - Leading Edge distributes Michaelangelo virus (PGN)
  - Re: Printer viruses, etc. (Mark Thorson, Ray Trent, Andrew Klossner, Jerry McCollom, John Stanley)
  - Re: Caller ID change of heart (Lance J. Hoffman)
  - Re: Snooping ... (Bob Frankston, Les Earnest)
  - <u>Re: Automated bill collectors, privacy, ... (Christopher Stacy)</u>
  - Credit cards at gas pumps (Mike Keeler)
- Issue 08 (28 January 1992)
  - "Stolen Identity" (Chris Hibbert)
  - <u>Unsafe artificial neural networks (Bill Armstrong)</u>
  - Re: A320 crash (Marc Horowitz, Christopher Ritter, Joel Upchurch, Scott Traurig, Jerry Bakin)
  - Re: Gulf war virus? (Paul Fellows, Ralph Moonen)
  - Re: Military uses for viruses (Don Tyzuk, Flint Pellett, Gene Spafford)

Re: A Tale of Risk Avoidance [so far ...] (Mark Thorson)

- Backup Systems and Marginal Conditions (Mike Bell)
- Risky Warranties (Jerry Hollombe)
- Issue 09 (1 February 1992)
  - Confusing Telephone System Overload Message (Bruce McCulley)
  - Re: Airbus A-320 (Helen Trillian Rose, anonymous, Harry Erwin, Joe Morris, Dave L. B., James B. Shearer)
  - Communication between ATC and pilot (lan Moor)
  - Another hacking myth (Robert Jenkins)
  - World Bank Virus [anonymous]
  - <u>Australian Tax File Numbers (Barry Johnson)</u>
  - Error in 1099-G Tax Form (William Mihalo)
  - Computer evidence is Hearsay (Kevin Stock)
  - The absence of a warranty (Fred Gilham)
  - Re: A Tale of Risk Avoidance [so far ...] (Rick Smith)
  - Serious dangers in the Caltrans AVI spec (Phil Agre)
- Issue 10 (3 February 1992)
  - Ballad of Silicon Slim (Cliff Stoll)
  - IRS quick refund by computer pays off -- like an errant slot machine (PGN)
  - Dutch crackers arrested (Wietse Venema via Cliff Stoll)
  - <u>'Virus' in Lithuanian Atomic Power Plant (Debora Weber-Wulff)</u>
  - <u>``All Bugs are Viruses'' (Chuck Lins)</u>
  - Supreme Court's mistaken fax (Clifford Johnson)
  - Lack of Integrity in the "real world" (Ted Lee)
  - Historical perspective on fault-tolerant architecture (Paul Eggert)
  - Re: Communication between ATC and pilot (Henry Spencer)
  - Re: Confusing Telephone System Overload Message (Bill Mahoney, Jay Schmidgall, Peter Desnoyers)
  - Re: Computer evidence is Hearsay (Ken Tindell, Robin Fairbairns)
  - Re: Warranties (Irving Chidsey, Charlie Mingo)
- Issue 11 (5 February 1992)
  - Dutch Hackers in Jail (Rop Gonggrijp)
  - Managing Director Job Announcement for CPSR (Eric Roberts)
  - <u>Contribution on A320 FMSs (Robert Dorsett)</u>
- Issue 12 (7 February 1992)
  - Another Radiotherapy Error (Brian Randell)
  - Aviation Software Certification (Brian Randell)
  - Our database says you'll read this item (Rodney J. Hoffman)
  - New England Telephone Refiles For CLASS Without Caller ID (John R. Covert)
  - US Sprint offering phone fraud insurance (Jonathan Allen)
  - Telephone hacker to be tried (Mark Seecof)
  - Dutch Crackers Shifting Blame? (Dave Pipes)
  - War on Drugs Communications Network Stalled (Sanford Sherizen)
  - Relative accuracy of FMS/INS navigation (Clifford Johnson, Robert Dorsett)
  - Strasbourg A320: Duck writes in Duck (Pete Mellor)
  - Re: Ballad of Silicon Slim (Laurence R. Brothers)
- Issue 13 (8 February 1992)
  - What next pizza over UUCP? (Peter J. Scott)

Re: New Caltrans AVI spec (Chris Hibbert)

- Re: Dutch police arrest hackers (Martin Minow)
- Re: Confusing Telephone System Overload Message (David Shepherd)
- Re: Radiation underdosages (Nancy Leveson)
- Re: Another Radiotherapy Error (Don Tyzuk)
- Re: Le Canard Enchaine (Bertrand Meyer, Charlie Mingo)
- VIRUS WARNING DaVinci Discovers Michelangelo (PC) (Kenneth R. van Wyk)
- CERT Advisory Michelangelo PC Virus Warning (CERT)
- <u>Michelangelo & the "Fix" Utilities (A. Padgett Peterson)</u>

## Issue 14 (16 February 1992)

- Police Foil Million Pound Hacking Plot (Ed Urbanowicz)
- Phone May Trap Kidnapper (Antony Upward)
- <u>Australian Government Bungles Private Data (Les Earnest)</u>
- Third Chicago Airport Selection (William E. Mihalo)
- Carpal Syndrome reports rise sharply (Jeff Helgesen)
- Patent Foul-up (Laurence Leff)
- Computer Virus Catalog: Jan.1992 edition (Klaus Brunnstein)
- Re: Dutch police arrest hackers (Brinton Cooper, Martin Minow)
- Automated Phone Systems (Michael J. Clark, via Allan Meers) [Humor]
- International finance (David B. Benson)

## Issue 15 (18 February 1992)

- <u>PCs and airline toilets (Craig Partridge)</u>
- Phone May Trap Kidnapper (Antony Upward) [Text missing from RISKS-13.14]
- Re: Police Foil Million Pound Hacking Plot (Bob Frankston, PGN)
- <u>Re: Carpal Syndrome reports rise sharply (Elizabeth Willey)</u>
- Risks in idle time (G. Sawitzki)
- <u>Risks in book buying -- shareware (Linda Stefny Baum via Bill Putnam)</u>
- <u>Prescription drug plan "benefits" (Jim Purtilo)</u>
- Re: Radiation underdoses (Jon Jacky)
- <u>Re: System certification again (Re: Radiotherapy) (Rick Smith, Marc Horowitz, Perry E. Metzger, Rich Kulawiec)</u>

## Issue 16 (24 February 1992)

- <u>Computer causes Olympics scoring error (David Shepherd)</u>
- Strasbourg Airbus crash report leaked (James Paul)
- More on Privacy in Australia (Bruce Howarth)
- Italian crooks let others pay phone bill (Debora Weber-Wulff)
- <u>Risk of Voice Mail Command Choices (Randall C Gellens)</u>
- RISCs of AP news reports (John Sullivan)
- Proposal for policy on calculator use during exams (Todd M. Bezenek)
- The Worth of Computing (Tony Buckland)
- <u>Computer Hackers Get Into Credit Records (Joe Brownlee)</u>
- VT Caller ID Decision (Marc Rotenberg)
- <u>Carpal Syndrome reports rise sharply (Brinton Cooper)</u>
- <u>Re: System certification again (Dave Parnas)</u>
- <u>MBDF Macintosh virus (Tom Young)</u>
- FBI Eavesdropping Challenged
- Issue 17 (25 February 1992)
  - California data-privacy/comp.crime bill [PART ONE] (Jim Warren)

- Issue 18 (25 February 1992)
  - California data-privacy/comp.crime bill [PART TWO] (Jim Warren)
- Issue 19 (27 February 1992)
  - The long arm of the law fingers old fingerprint (PGN)
  - \$300,000 budget error at The Whig Standard (Jim Carroll)
  - Patriot missiles misled by `accidental' decoys (Lord John)
  - More on the Airbus A320 (Andrew Marchant-Shapiro)
  - Re: Italian crooks let others pay phone bill (Ralph Moonen)
  - <u>Two Cornell Students Arrested for Spreading Virus (PGN)</u>
  - Re: Calculator Use During Exams (Bob Frankston, Brinton Cooper, Li Gong, Jeffrey Siegal, mathew)
  - Re: Carpal Tunnel Syndrome etc. (Steve Bellovin, Brinton Cooper, Ralph Moonen, Jeremy Barth, Simona Nass, Brinton Cooper, Torsten Lif, Claire Jones)
- Issue 20 (28 February 1992)
  - Risks of poor design (IRS Teletax phone system) (Andrew Marchant-Shapiro)
  - Digital RF Link at 2 Mbps Wireless Monitoring (Joe Jesson)
  - Overly curious exhibit at Chicago museum (Karl Swartz)
  - CallerID for PC's (Jonathan D Arnold)
  - International Cooperation on Computer Crime and Extradition (Sanford Sherizen)
  - Re: More on the Airbus A320 (Robert Dorsett)
  - Re: The long arm of the law fingers old fingerprint (Brinton Cooper, PGN)
  - Re: Calculators in exams (Robert J Woodhead, Espen Andersen, Mark Jackson, Joe Morris, Mark Kantrowitz)
  - \*\*\* DIAC-92 \*\*\* (Douglas Schuler)
- Issue 21 (2 March 1992)
  - Leap year strikes again (Lee Laird via Jaap Akkerhuis, Mark Brader, Rob Slade, Paul Eggert)
  - Leap day liquor licence problem (Douglas W. Jones)
  - <u>Another Happy Story (Alan Wexelblat)</u>
  - Montreal Life Insurance company destroyed by computer errors? (Peter Deutsch)
  - Post Office uses only 7 characters to disable my husband's ATM card (Christine Piatko)
  - Not quite anonymous FTP (William Rucklidge)
  - Virus news-bite omits crucial information (jcav)
  - Scud vs Patriot (Peter G. Neumann)
  - Re: More on the Airbus A320 (Pete Mellor, Peter Ilieve)
- Issue 22 (3 March 1992)
  - RISKS in Test Standards -- A 900,000-mile Oldsmobile? (Andrew C. Green)
  - ATMs gobble bankcards in Colorado (Rex E. Gantenbein)
  - Re: Virus news-bite omits crucial information (Vesselin Bontchev)
  - Re: Not quite anonymous FTP (Jonathan I. Kamens)
  - FLIGHT INTERNATIONAL on A320's VOR... (Robert Dorsett)
  - <u>RSA Laboratories announces RSAREF free cryptographic toolkit (Burt Kaliski)</u>
- Issue 23 (3 March 1992)
  - Leap Day bug hits PC mail program (Roger H. Goun)
  - Software Virus Found At INTEL
  - Re: Michelangelo platforms (Sean Eric Fagan, Brandon S. Allbery)
  - Re: RSA Laboratories announces RSAREF (Marc Horowitz, Burt Kaliski)
  - New Caltrans AVI spec (Phil Agre)

- Re: Post Office uses only 7 characters ... (Craig Seidel)
- Re: Not quite anonymous FTP (Mike Pabrinkis)
- Re: More on the Airbus A320 (Martyn Thomas, Robert Dorsett, Ed Hutchins, Pete Mellor, Bob Kerns perhaps)
- Issue 24 (4 March 1992)
  - Orange County Must Delay Stormwater Tax (Tanner Andrews)
  - Major software problems at TSE (Mark [with note from Bjorn Freeman-Benson])
  - Garbage In, Gospel Out -- genetic info (Vivek Khera)
  - 1-900 spelling game (Andrew Tannenbaum)
  - AT&T's operatorless collect calls (PGN)
  - Private SS Data Sold to Information Brokers (Chuck Lins)
  - RISKS of international trade negotiations: intellectual property, patents (Jyrki Kuoppala)
  - A320 and significance (Henry Spencer)
  - MAGSAV bug explained (Paul Eggert)
  - Re: Leap year strikes again (Rhys Weatherley)
  - <u>Re: RSAREF license (David L. Black)</u>
  - <u>Re: Viruses (Bob Frankston)</u>
  - Re: Virus news-bite omits crucial information (John Cav..., A. Padgett Peterson, Steve Milunovic).
- Issue 25 (5 March 1992 [issued with erroneous SUBJECT: RISKS 13.26])
  - Sizewell (and RISKS) on UK TV (Perry Clarke)
  - Musical risks (Geoff Kuenning)
  - <u>``Helpful'' self-configuring programs (Steve Bellovin)</u>
  - A RISK architecture? (DEC's Alpha) (Sites/Witek quoted by Brian Randell)
  - Re: Private SS Data Sold to Information Brokers (Jerome H Saltzer)
  - Re: 7-character PO key (Christine Piatko, Jenn Turney, Irving Chidsey, Dan Hankins)
  - <u>Repetitive stress injuries (Steve Bellovin) [longish]</u>
- Issue 26 ([sic] 6 March 1992)
  - Name this risk... [Primative logic] (Michael Travers via Rex Black)
  - Mouse restrictions on American Airlines (Bob Frankston)
  - Exporting Apples (Burt Kaliski, RSA Laboratories)
  - Bargain Harold finds computers no bargain (Dave Wortman)
  - Re: Sizewell (and RISKS) on UK TV (Pat Place)
  - Risks of Automated Phone Operators (Charles Olson)
  - <u>Speed-droid tickets junked car (Jane Beckman)</u>
  - <u>Risks of Barcoded money (Mark Gonzales)</u>
  - <u>Safeway "Frequent Shoppers Club" (Jeremy Epstein)</u>
  - Re: Musical Risks (Katz, rwk)
  - Re: Bureau of Centralization -- Phone Taps (Peter Wayner, Steve Dever)
  - New Legislation on Computer Security (Lance J. Hoffman)
  - Re: Michelangelo (anonymous, Graham Mainwaring)
  - Technical terminology -- and viruses (Brian Rice)
  - Re: A RISK architecture? (DEC's Alpha) (Steve Bellovin, Tom Blinn)
  - Imprecision not considered harmful (Eric Sosman)
- Issue 27 (7 March 1992)
  - Re: Michelangelo reports (Robert Slade, Bill Murray, David Leslie, Brandon S. Allbery)
  - (Mis)perceptions of RISKS (Steve Strassmann)
  - Re: Lap Mice (Steven Wilson, Bill Murray, Robert L. Smith)
  - RISKS in the news -- recharging portables (Stephen C. Woods)
  - Re: A RISK architecture? (DEC's Alpha, IBM 360/91) (Andrew Klossner, John R. Levine, Melvin Klassen)

- Electronic privacy in California (Phil Agre)
- Re: 1-900 spelling game (David C. Martin)
- Re: A320 (Paul Wallich)
- Re: 7-character PO key (Jonathan Griffitts)
- Issue 28 (16 March 1992)
  - "British plug in" (Grant Grundler)
  - Airport parking is expensive, but... [this is ridiculous] (Tsutomu Shimomura)
  - <u>Computer-Aided Robbery at Clydesdale Bank (Brian Randell)</u>
  - X-15 reliability experience (Henry Spencer)
  - Fly-by-wire SAAB (Brian Randell)
  - Corporate Strategies for Info Protection, Ethics, Privacy (Sanford Sherizen)
  - RISKS backlog (PGN)
  - <u>Re: American Mice (Mouse interference) (Scott Colwell, Rob Warnock, Craig, Brian Rossmajer,</u> <u>Bob\_Frankston)</u>
  - Registration for IEEE SRSP (Research in Security and Privacy) (Liz Luntzel)
- Issue 29 (18 March 1992)
  - Risks of success vs risks of failures elsewhere -- Magellan turnoff? (PGN)
  - Shocking news: computer models sometimes inaccurate (Jeffrey Mogul)
  - <u>New RISK at Railroad Crossing Gates (Alan Marcum)</u>
  - <u>Microsoft Word 5.0 install risk (W.M. Buckley)</u>
  - It has easy written all over it -- printing envelopes (Brian Kantor)
  - <u>Airport door magstrip security (Mark Seecof)</u>
  - ITSEC V1.2 Observations by German GI Task Force ... (Kai Rannenberg)
  - FOLLOWUP: NASA hacker sentenced (Bear Giles)
  - Wiretapping and ISDN (Frank Heath, I.Wakeman via Olivier M.J. Crepin-Leblond)
  - Bugging ISDN (Torsten Lif via John Gilmore)

## Issue 30 (23 March 1992)

- Globex fails critical test (PGN)
- Error in math chips away at ice storm aid (Marty Leisner)
- Two Risk Phenomena: Atari blanks, Turbo Pascal clocks (Stefan Burr)
- Virus breaks security of Italian Judicial System's computers (Miranda Mowbray)
- Re: Why Microsoft wants you to turn off virus checkers (Martin Minow)
- New RISK at Railroad Crossing Gates (Bill Gripp, David Flanagan)
- <u>Re: Magellan Turnoff (David Fetrow)</u>
- Human Rights Groups Armed (With Technology) (Sanford Sherizen)
- Saab fly-by-airbags and roaring mice (Andrew Klossner)
- UA 747 Lost Door; Broadcasting mice (Bob Frankston)
- A comment on naivete (Bob Frankston)

## Issue 31 (27 March 1992)

- <u>New XEROX FAX software (Jeremy Epstein)</u>
- FYI: Congressional Advisory Board calls for public review (Jim Warren)
- <u>Re: Microsoft and virus checkers (Alan Wexelblat)</u>
- <u>Dumbing down new systems (Lance J. Hoffman)</u>
- The FBI Needs Industry's Help--OpEd in NYT (Kurt F. Sauer)
- Accidental stock sale: The error crept in when ... (Bob Frankston)
- U.S. Dept. of Justice Rulings about Keystroke Capturing (Sanford Sherizen)
- <u>Test data used for actual operation once again (Bertrand Meyer)</u>
- <u>Re: UA 747 Lost Door (Brian Boutel)</u>

## Issue 32 (1 April 1992)

- Pentagon homes in on Patriot critic (Lord John Wodehouse)
- Overly clever failsafe system (Mark Bartelt)
- Now why didn't I think of that? (Windows 3.1) (J Chapman Flack)
- Re: U.S. Dept of Justice Rulings about Keystroke Capturing (Tom Zmudzinski)
- Re: Dumbing down the FBI (Janlori Goldman via Daniel B. Dobkin, Brian Kantor, Dave Banisar via Lance Hoffman, Heather Hinton)
- <u>Conference Announcement: DIAC-92 (Pavel Curtis)</u>

## Issue 33 (2 April 1992)

- William Gibson, An (On-Line) Book of the Dead (PGN)
- NSA and cryptographic software (PGN)
- US Navy radar jammers pass test despite software errors (Jay Brown)
- SDI (from Newsweek) (John Sloan)
- <u>A remarkably stupid design decision (Geoff Kuenning)</u>
- <u>Risk of "parameter validation" hype (Mark Jackson)</u>
- Re: FBI v. digital phones (Daniel B. Dobkin)
- Re: Laws to Ease Wiretapping (A. Padgett Peterson)
- <u>Re: Aviation Software Certification (Brian Randell)</u>
- WAR GAMES II (Eric S. Raymond)
- Issue 34 (3 April 1992)
  - Re: SDI (David Parnas)
  - Re: NSA and cryptographic software (Steve Bellovin, Fred Cohen)
  - <u>Risks in nuclear bombs to deflect asteroids (Marvin V. Zelkowitz)</u>
  - <u>The new Simon & Schuster Royalty Accounting System (Lauren Wiener)</u>
  - Bad data allowed to enter driver database and used as basis for arrest (Eric Postpischil)
  - Re: U.S. Dept of Justice Rulings about Keystroke Capturing (Marc Horowitz, Thomas Zmudzinski)
  - RISKS of patents on software, ideas, etc. (Bob Estell)
  - Backup over the phones? (Robert Ebert)
  - Re: Now why didn't I think of that? (Windows 3.1) (James Barrett)
  - The Machine That Changed the World -- Public TV Series (Jack B. Rochester)
- Issue 35 (4 April 1992)
  - Some details on Patriot problem (Frederick G. M. Roeber via Stanley Chow)
  - Re: War Games II (Les Earnest)
  - More on Gibson electronic book virus (Tom Maddox via Blake Sobiloff)
  - <u>Re: Neuromancer (Keith Bierman)</u>
  - Risks of faked-up software advertising (John Lupien)
  - Xerox PaperWorks; Imprecise Interrupts (Barry Johnson)
  - Imprecise FP traps (Gideon Yuval)
  - CMOS RAM for security (Tom Brusehaver)
  - Subject of the Data as "Owner" (Bill Murray)
  - Re: FBI v. digital phones (Cris Pedregal Martin)
  - On Electronic Privacy... (Peter Wayner)

## Issue 36 (6 April 1992)

- More Glitches in Time -- and Gambling profits (anonymous)
- X400 (Cliff B Jones)
- Re: Good crypto (Fred Cohen)

## Correcting Erroneous Database Listings (Steven S. Davis)

## Issue 37 (9 April 1992)

- Fremont CA Air Traffic Control Center Outage (PGN)
- The Army reflects on the Patriot (PGN)
- Risks of on-line documents dated April 1 (David Tarabar, Robert Ebert)
- <u>Rounding error changes Parliament makeup (Debora Weber-Wulff)</u>
- Believe it or not -- there's some reason on the bench! (Phil R. Karn)
- <u>Cryptography used by Terrorist Organisation (Kees Goossens)</u>
- <u>Crypto (Export) Policy (Bill Murray, Brinton Cooper)</u>
- <u>Certification of Cockpit Automation (John Theus)</u>
- The Paper(less) Trial (J Chapman Flack)
- <u>Risks of academic cheating by computer (Prentiss Riddle)</u>
- Public TV series revisited (Brian Tompsett, Nick Rothwell)
- <u>Re: Correcting Erroneous Database Listings (Fred Gilham)</u>
- Software Failures (Lin Zucconi, PGN)

## Issue 38 (10 April 1992)

- <u>New California lottery game delayed by program flaw (PGN)</u>
- High Marks & Spencer -- it's-pence'r-pounds (Dorothy R. Graham via PGN)
- London Ambulance Service computer system problems (Dorothy R. Graham via PGN)
- Women's lives imperiled by medical software (Dorothy R. Graham via PGN)
- <u>Computer "error" blamed for murder? (PGN)</u>
- U.S. Justice Dept.'s Alien Deportation Notification File Prototype Inaccurate (Sanford Sherizen)
- <u>Re: Killer Asteroids, Detect/Deflect (Tom Neff, Leslie DeGroff)</u>
- FBI phone taps (Mark Seecof)
- Data compression & American cryptographic export policy (Conrad Hughes)
- Re: Cryptography used by Terrorist Organisation (Dik Winter)
- PBS TV Show Accuracy (R.Y. Kain, Dave Marvit for WGBH-TV)
- The makers of the PBS series respond (Dave Marvit)
- <u>Computer Users Foil Virus (Don Clark via PGN)</u>
- Issue 39 (13 April 1992)
  - Federal Reserve Bank snafu delays bank deposits (PGN)
  - <u>St. Petersburg issues credit cards to protect bank deposits (PGN)</u>
  - The Tyranny of Truncation (Mark Jackson)
  - Re: U.S. Dept of Justice Rulings about Keystroke Capturing (Jim Griffith)
  - Re: Risks of on-line documents dated April 1 (Robert Ebert)
  - Re: Tapping phones, encrypting communication, and trust (Jerry Leichter)
  - FBI Phone Taps (George Yanos)
  - Fuzzy logic in cars (PGN)
  - <u>Compression and Encryption (Douglas W. Jones)</u>
  - Re: Telephone system foibles (James Zuchelli)
  - Risks of Friends and Family (Fred Cohen)
  - Re: The makers of the PBS series respond (Brian Tompsett)
  - Re: Correcting Erroneous Database Listings (Steven S. Davis)
  - Query: academic transcripts (William Nico)
  - Microsoft Windows(tm) 3.1 write cache (Andrew Birner)

## Issue 40 (15 April 1992)

- <u>Risk of relying on editors and/or spelling checkers? (Siritzky)</u>
- New Applications of Voice Recognition Technologies (Saul Tannenbaum)

- For savings we can count on our fingers... (Jeffrey Sorensen)
- Computerized insurance quotes (Bear Giles)
- Re: Risks in nuclear bombs to deflect asteroids (Dani Eder)
- Re: Unauthorized Evidence Gathering (Peter K. Boucher, anonymous)
- Re: Phone Registration at Berkeley (Eric W. Anderson)
- Re: Transcripts via e-mail (Dick Kain, Shyamal Jajodia)
- Re: Public TV Series (Wayne Throop, Dave Katz,
- Re: US PBS stations \*do\* censor (Jonathan Clark, Matt Braun)

#### Issue 41 (16 April 1992)

- <u>Re: Tapping/taping (Donn Parker, Mark Rasch, Joel Upchurch, Phil Karn, Mike Gore, John Mainwaring, Irving Wolfe)</u>
- FBI phone tapping bill (Steve Dever)

#### Issue 42 (19 April 1992)

- Chicago has a single point of failure (Bryan MacKinnon)
- Re: FAA crash (Howard Israel)
- More delays at East Bay air traffic control center (PGN)
- Drugs by EMail (PGN)
- Potentially disastrous bug in MacInTax (Edgar Knapp)
- Automagically generated phone books (PGN)
- Re: Risks of editors -- Mass Pike (Carl Ellison)
- Re: Long call wait for London Ambulances (Brian Tompsett)
- Re: FBI wiretaps (Eric S. Raymond)
- <u>Re: Intercept legislation (Bob Weiner, Donn Parker)</u>
- Credit-card fraud (Bruce Bigelow and Dwight Daniels)
- Harper's article on Personal Data for Sale
- SURVEY: Is Big Brother Watching You? (Lorrayne Schaefer)

#### Issue 43 (22 April 1992)

- Typos? They've been around for centuries! (Cliff Stoll)
- Phantom ATM withdrawals (Lord Wodehouse)
- Re: Potentially disastrous bug in MacInTax (John Stanley)
- Re: Risks of too-subtle April Fools Jokes (Pete Mellor)
- Re: Long call wait for London Ambulances (Lord Wodehouse)
- A New Species in the Food Chain (Ruth Bork)
- <u>Re: FBI and telephones (James Zuchelli)</u>
- Re: Telephone Foibles (James Zuchelli)
- More on electronic anklet (Brinton Cooper)
- Michelangelo Avoidance report (Klaus Brunnstein)
- Congressional Vote & The Electronics Industry (Philip Greenspun via Carl Baltrunas & Cherie Marinelli)
- Industrial Strength Formal Methods -- Call for Papers (Cliff B Jones)
- Issue 44 (27 April 1992)
  - An "Own Goal" by the RAF (Brian Randell)
  - Risks of a modern weatherman (Bear Giles)
  - <u>Standard deviation in LOTUS 1-2-3?! (Lord Wodehouse)</u>
  - Ralph Nader/Cable TV/Information Networks (Ralph Nader and Jim Donahue)
  - <u>Re: Tax on computer media (Mark Seecof)</u>
  - Tracking by Cellular Phone (Brian Kush)
  - Re: Admissibility of video tapes (Craig R. Smilovitz)
  - Voice mail security (Richard Dickson)

- Re: Bugging Phone Calls (Jay Denebeim)
- Re: Tapping Bill (Allen Smith)
- Re: FBI and telephones (Bob Frankston)
- Puzzle-box patent abandoned (Ross Williams)

## Issue 45 (28 April 1992)

- Software observing daylight savings time when it \*shouldn't\* (Mike Morton)
- Is it getting too easy? (Spreadsheetology) (Robert Slade)
- IEEE/CS Workshop on Ethical Standards for the Profession (Jim Horning)
- FBI and Mailing Lists (Mary Culnan)
- <u>Re: Voice mail security (Dan Wing)</u>
- Re: Tracking by cellular phone (John Karabaic, Phillip. D. Brown)
- <u>COMPASS '92: Conference on Computer Assurance (Laura Ippolito)</u>

## Issue 46 (2 May 1992)

- F-22 crash (Barton Gellman via Nancy Leveson)
- Dean's password used to misappropriate funds (Janet M. Swisher)
- <u>April fool meteorology (Bob Grumbine)</u>
- <u>Patriot: The missile that missed (Lord Wodehouse)</u>
- Re: Ralph Nader/Cable TV/Information Networks (Tom Wicklund)
- AT&T announces Easy Reach 700 (PGN)
- Re: Tracking by Cellular Phone (Les Earnest, Mark Fulk, Kevin Paul Herbert)
- Free TRW Credit Report (Mary Culnan)
- Shut Down Ambulance Computer (Jean Ramaekers, Scott Dunham via Lord Wodehouse)
- Risks of using cash (Robert Ebert)

## Issue 47 (7 May 1992)

- \$70 million bank scam (PGN)
- Insurance Computer Can't Handle Twins (Ed Ravin)
- High-tech software + low-tech hardware == network failure (Jonathan Hardwick)
- Secure phones easily available (Alexis Porras)
- Re: F-22 crash (Robb Watson)
- Re: Free TRW Credit Report (Jack Holleran, Dave Turner)
- Issue 48 (10 May 1992)
  - Farmer receives \$4M US Government check by mistake (Fernando Pereira)
  - Daylight savings time started early this year (David J. Fiander)
  - C-17 software problems (Mark Seecof)
  - Composite Health Care System at Walter Reed Hospital (PGN)
  - <u>Microsoft advocates killing of Jews (Aaron Dickey via Jim Horning)</u>
  - DATATAG (Brian Randell)
  - Re: \$70 million bank scam (Tom Perrine)
  - <u>Re: April Fools' Meteorology (Bear Giles)</u>
  - Re: Free TRW Credit Report (Mary Culnan)
  - <u>Risk of direct deposit (Stuart Bell)</u>
- Issue 49 (16 May 1992)
  - Shuttle computer miscomputes rendezvous (John Sullivan)
  - <u>The computer made me do it! [Brain enchipment] (Bear Giles)</u>
  - <u>NY Times Columnist Protests Efforts to Prevent Secure Communications (Peter D. Junger)</u>
  - <u>New York Times Computer Typesetting (Craig Partridge)</u>

Lack of FTP warning "destroys" hard drive (Taed Nelson)

- Ankle bracelet; a busy phone ==> scott-free (McGrew)
- No access to exchange via Cellnet (Lord Wodehouse)
- OTA has issued a report re "software property" (Jim Warren)
- Pentagon taps hackers to write viruses (John Mello)
- Re: Microsoft advocates killing of Jews (Mathew)
- Two privacy newsgroups [Don't confuse them.] (PGN)
- Announcing the PRIVACY Forum digest! (Lauren Weinstein)
- Computer Privacy Digest/comp.society.privacy (Dennis G. Rears)
- MDC, the C-17 and the F-15E (John Karabaic)

## Issue 50 (17 May 1992)

- Food stamp computer misbehaves in Maryland (Joseph E. Richardson)
- Spelling checker advocates massive drug abuse (Randy Lindsey)
- Credit card databases prefer St. to zip codes (David C. Kovar)
- Risk of TRW Not Having Enough Information (S. Peter Loshin)
- <u>Re: Free TRW Credit Report (R. R. Hauser)</u>
- Yet more Software-in-the-Air scares (Simon Marshall)
- More on the F-22 crash: pilot error now blamed (PGN)
- Re: F-22 crash, cont'd. (Daniel P. Johnson, Larry, Bob Rehak)
- Final Announcement for IFIP/Sec '92 (Guy G. Gable, Carlos Delgado Kloos)
- FTC Newsletter Volume 9 (FTCS-92 + workshop on Fault-Tolerant Par.Dist.Sys.)

#### Issue 51 (20 May 1992)

- Autopilot Flaw (Jaap Akkerhuis)
- GAO report on C-17 software (James Paul)
- Big Brother in The Netherlands (Jan L. Talmon)
- Keystroke capture (Mark Rasch)
- <u>Risk of serving lunch to the First Lady (Timothy Petlock)</u>
- Re: TRW (Willis H. Ware)
- comp.risks WAIS servers available (Scott Draves)
- Re: Not enough trained computer experts (Fred Cohen)
- Re: Yet more Software-in-the-Air scares (Pete Mellor, Martyn Thomas)
- REMINDER on COMPASS '92: Conference on Computer Assurance (Laura Ippolito)

#### Issue 52 (27 May 1992)

- Yellow Slime Shuts Down Munich Opera (PGN)
- "Programming error" prevents long distance billing (Bob Robillard)
- White House Fights to Erase E-Mail Backups (Randy Gellens)
- <u>Critical technologies (Martyn Thomas)</u>
- Re: Not enough trained computer experts (Robert Dorsett)
- <u>Provisional program DCCA-3 (Luca Simoncini)</u>
- Issue 53 (30 May 1992)
  - Software problem in shuttle software (Nancy Leveson)
  - The Thin Edge of the Wedge? Next-of-kin database in Vienna VA (Barry Johnson)
  - The Federal Government and Civilian Encryption (Larry Hunter)
  - White House records (E. N. Kittlitz)
  - <u>Computer virus insurance (John Mello)</u>
  - The risks of telling the truth about viruses (Fred Cohen)
  - C-17 problems attributed to software diversity (David G. Novick)
  - C-17 story, Chmn. McDonnell's reply (via Michael Cook)

- SDI Costs (anonymous)
- <u>Risks of SDI? (PGN)</u>
- New CPSR List Server (Ronni Rosenberg)
- Call for Papers, IFIP/Sec '93 (Dr. Harold Joseph Highland)
- Issue 54 (3 June 1992)
  - Risks of Space Junk (PGN)
  - Girl killed in automatic car window (Ian Spalding)
  - Pepsi promotion error blamed on computer glitch (Roland Ouellette)
  - <u>Voter-registration computers know best (Les Earnest)</u>
  - (more) Social Security Numbers -- billing overloads (Mark Bergman)
  - <u>Reverse Passwords? (Brinton Cooper)</u>
  - Risks of being a computer-font company president? (PGN)
  - Re: Shuttle computer miscomputes rendezvous (Randall Davis)
  - Re: The risks of telling the truth about viruses (Theodore Ts'o)
  - <u>Re: Yellow slime (PGN)</u>
  - Re: Critical technologies (Martyn Thomas)
  - Re: Payphone Xenophobia (roeber via Darren Alex Griffiths)
  - Re: Not enough trained computer experts (Brinton Cooper and Fred Cohen)
- Issue 55 (5 June 1992)
  - The sinking of the trawler "Antares" (Brian Randell)
  - Another "But I'm Not Dead" story (Bill Winn)
  - <u>\*67 TOGGLES calling-number-id blocking (Bob Frankston)</u>
  - One-Armed Bandits? (Bob Frankston, Roland Ouellette)
  - Girl Kidnaped by her Computer! (Misinformation About Computers) (Ellen Spertus)
  - Re: Girl killed in automatic car window (David Parnas)
  - Barry's Bug (Eric Haines)
  - German Unification Breaks Ohio Bell's Billing System (Adnan C. Yaqub)
  - Human namespace collisions (Frederick G. M. Roeber)
  - A name is a name is a name (Rick Simkin)
  - "Benevolent" Viruses (A. Padgett Peterson)
  - Software in the Air Scares: CAA and article authors respond (Simon Marshall)
- Issue 56 (9 June 1992)
  - Vote-by-telephone disaster in Nova Scotia (Daniel MacKay, Richard P. Taylor)
  - Computer Injury and Product Liability -- RSI (Gary Chapman)
  - Printer `ruined firm' (Paul Leyland)
  - BBS Fraud (Tokyo) (Shaun Lawson)
  - Endeavour rendezvous software fix (James Paul)
  - ACM TOSEM mailing label problem (David Lamb)
  - Re: Slot Machines, etc. (Tom Watson)
- Issue 57 (10 June 1992)
  - Perot computers cracked (Larry Hunter)
  - \$150 printer hangs \$0.5M VAXcluster (Marc Shannon)
  - Reviewing Communications in the Gulf War (James Paul)
  - Endeavor bug -- more details (Nancy Leveson)
  - <u>Where on earth are you? (Richard Murnane)</u>
  - <u>Risk of Computer Generated Fund-Raising Letters (Lee Hasiuk)</u>
  - <u>Car computer downloading (Bob Sidebotham)</u>
  - Telecom Australia allows easy denial of service attack [anonymous]

- Follow-up to Dead Driver story -- PennDOT replies (Mike Berman)
- Re: BBS Fraud (Fred Gilham)

## Issue 58 (15 June 1992)

- SoundWars: SW Sabotage, Creative Technology vs. Media Vision (PGN)
- FBI raid on bulletin board (Gary Chapman)
- NY TIMES MAGAZINE story on defects in personal computer software (Jon Jacky)
- <u>Computer system refuses large deposit (Richard Frantz Jr.)</u>
- Delivery Failure in a Paging System (William Griswold)
- Update on vote-by-telephone disaster in Nova Scotia (Daniel MacKay)
- <u>Risks of not foreseeing supplement and maintenance funds (Geraldo Xexeo)</u>
- Re: Follow-up to dead driver (Michael Favor)
- Re: Where on earth are you? (Scott Traurig)
- Re: Car computer downloading (Bruce Oneel)
- Re: Perot computers cracked (Steve Bellovin, Joe Morris)
- Product risks (Re: Parnas, Girl killed in automatic window)(Bergtor Skulason)
- Online Symposium: Visions for a Sustainable World Pugwash Conference (Jeffrey Porten)
- Issue 59 (18 June 1992)
  - SOUNDEX algorithm fails in Directory Enquiries (Nick Rothwell)
  - Two wrongs make a right (Fred Cohen)
  - <u>Computer problem provides free phone porn (Mark Bartelt)</u>
  - Australia benefits from US encryption export ban (Rick Noah Zucker)
  - <u>Re: Missed Pagings (Marc Schwartz)</u>
  - Privacy problems with voter records (Norman Kraft)
  - Call for Participation, CFP '93 (Bruce R Koball)
- Issue 60 (1 July 1992)
  - Houston Chronicle Crypto Article (Joe Abernathy)
- Issue 61 (1 July 1992)
  - The NSA Papers (Joe Abernathy)
- Issue 62 (4 July 1992)
  - Emergency system fails -- Risks of firing employees? (Jim Griffith)
  - Nutrasweet Telephone Sweepstakes (Ranjit Bhatnagar)
  - Risk of Assuming an Int will do (Russell Aminzade)
  - <u>Students cheated BT to win computerised phone contest (Philip Hazel)</u>
  - <u>Computer-literate children find porn (Andrew Shapiro)</u>
  - <u>UK ATMs legal challenge (Antony Upward)</u>
  - <u>CPSR Challenges Virginia SSN Practice (David Sobel)</u>
  - Are Humans Always Responsible for Computer Errors? (Peter Danielson)
  - Fokker F.100 incident (Robert Dorsett)
  - Another Fokker F.100 incident (Olivier Plaut)
- Issue 63 (8 July 1992)
  - <u>Newsweek Vincennes article (Bob Frankston)</u>
  - Are bank machines private? (Andre Bacard)
  - Virus consumes clerks at Sears (Kurt Guntheroth)
  - GI Observations on IT Security Evaluation Manual (ITSEM) V0.2 (Kai Rannenberg)
  - Voting by Phone in Nova Scotia (Evan Ravitz)

- When Cryptography is Outlawed... (Kurt Guntheroth)
- <u>Re: computer-literate children find porn (Karl Lehenbauer)</u>
- ESORICS 92: Preliminary Programme (Yves Deswarte)
- Issue 64 (14 July 1992)
  - RISKS (and CSL.SRI.COM) outage (RISKS)
  - <u>Phreaking/Blue Box program (Klaus Brunnstein)</u>
  - Five `Hackers' Indicted (PGN)
  - Huge credit card record theft uncovered (Norm deCarteret)
  - Risks quotation (Jonathan Bowen)
  - <u>Re: Newsweek Vincennes article (Dan Sorenson)</u>
  - Re: Airbus (Mark Brader and Keith Barr)
  - Re: When Cryptography is Outlawed... (Fran Litterio, Arthur L. Rubin)

#### Issue 65 (17 July 1992)

- NY "Hacker" Indictments (John F. McMullen)
- Questionmark over nuclear reactor control software (Anthony Naggs)
- Call for papers FTCS-23 (Mohamed Kaaniche)

#### Issue 66 (18 July 1992)

- Qantas airliner challenged by US Pacific fleet (Anthony Naggs)
- Residual Gulf war battle plans provide evidence of stolen computers (PGN)
- U.S. encryption export control policy softens somewhat (PGN)
- 911 call lands caller in jail (Mel Beckman)
- Re: Nuclear reactor control (Bill Park)

#### Issue 67 (22 July 1992)

- More identical name confusion (plus Scientific American item) (Mark Bergman)
- A computer as a criminal tool (Peter D. Junger)
- <u>American Airlines software development woes (Randall Neff)</u>
- RISKS of Antilock Braking Systems (David Palmer)
- RISKS of BBS ownership (David R. Cohen via Scott Bailey)
- The role of expertise in technological advances (Bertrand Meyer)
- Telephone wiretapping (E. Kristiansen)
- Bellcore threatens 2600 with lawsuit over BLV article (Emmanuel Goldstein)
- Re: Export of 40-Digit RSA (Dorothy Denning)
- Re: Qantas airliner challenged by US Pacific fleet (Leonard Erickson)
- Re: Nuclear reactor control (Rusty Teasdale)
- Re: Airbus -- Countering Urban Myths (Bjorn Freeman-Benson)
- <u>AVIATION restructuring in progress (Robert Dorsett)</u>

#### Issue 68 (23 July 1992)

- Telco problem with Garth Brooks concert ticket sales proves fatal (Art Corcoran)
- Re: 911 call lands caller in jail (SATRE)
- Re: A computer as a criminal tool (Jonathan A. Marshall)
- The onus of correcting databases (Henry G. Baker via PGN)
- Crypto systems -- less is more (Chaz Heritage)
- <u>Re: BBS Pornography (Chuck Stern, Art Corcoran)</u>
- Re: Bellcore threatens 2600 (Mel Beckman)
- 2600 reply to Bellcore lawsuit threat (Emmanuel Goldstein)
- Re: Technology and leading employees: another example (Clifford Johnson)

#### Re: Nuclear reactor control (Tom Ohlendorf)

#### Issue 69 (3 August 1992)

- <u>Computer scoring glitch at Olympics (John Carr)</u>
- <u>Wiretap Proposal Needs Study (Joe Abernathy)</u>
- UK Inland Revenue to be privatised? (Paul Johnson)
- 21st-Century Singapore (Bob Frankston)
- User interface studies: oh, what's the use? (Robert Slade)
- Re: More identical name confusion (anasaz!John)
- Re: 911 call lands caller in jail (Ed Ravin, Derek Beatty)
- Software Hazard Analysis Course (Gord Symonds)
- CPSR Recommends NREN Privacy Principles (Dave Banisar)

#### Issue 70 (6 August 1992)

- Software problems plague new Canadian air traffic control system (Mark Bartelt)
- Fun with high pressure (Michael Stern)
- Mr. C. Baggage, who was neither a Mister nor a Baggage at all (Geoff Kuenning)
- Unreliable call-return phone feature... (Rex Black)
- GTE's Personal Secretary (Chuck Ham)
- Police files (Nigel Allen)
- Re: User interface studies: oh, what's the use? (Steve Summit)
- <u>Sweet Old Things and User Interfaces (Ed Ravin)</u>
- Re: Computer scoring glitch at Olympics (Stanley Chow, Joe Konstan, David Wittenberg)
- 1993 Symposium on Research in Security and Privacy (Dick Kemmerer)
- Issue 71 (7 August 1992)
  - "Bug" or fraud? (John Kriens)
  - Ship with computer-controlled ballast tanks tips over (Jon Jacky)
  - Bugs in microcode of CPUs [REQUEST FOR EXAMPLES] (Brian A Wichmann)
  - <u>A problem with call waiting (Rick Pim)</u>
  - Phone service modification (Kraig R. Meyer)
  - Re: Unreliable call-return phone feature... (Joe Konstan)
  - Re: computer scoring at olympics (Jong, Gary McClelland)
  - Sweet Old Things and User Interfaces (Anton Martin Ertl)
  - Re: Mr. C. Baggage, ... (kennykb)
  - Information Age course at Georgetown (Ross Stapleton)
  - World Conference on Network Administration and Security (Hal Pomeranz)

#### Issue 72 (12 August 1992)

- Electronic Voting Machines Alert (Rebecca Mercuri)
- NWB credit-card errors affect millions (Philip Hazel, Jonathan Bowen)
- <u>Cash Card Fraud the public fights back (Brian Randell)</u>
- "Around the state at Barnett Banks, it did not compute" (Norm deCarteret)
- The QE2 and navigational charts (John Sullivan)
- Stupid computers--The Economist reports on AI (John Sullivan)
- GAO reports on NASA (James Paul via PGN)
- Re: Ship ... tips over (Cristobal Pedregal Martin)
- Re: Stupid things people do (Joseph F. Hull)
- <u>Re: Bug or Fraud (Michael Friedman)</u>
- <u>RISKS of DOS, Caller-ID, Voice Mail... (Peter da Silva)</u>
- Issue 73 (17 August 1992)

- Microwave oven autonomously turning on (A E Eckberg)
- Outdated sports news recurs (Geoff Kuenning)
- Fire department to get computer dispatching (Robert Allen)
- Electronic payment takes 2 weeks! (D. Langford)
- Security breach cited as class schedule erased (UBC) (Thomas Dzubin)
- A true tale of terror in the making: AUTOPAY (Steve VanDevender)
- Another saga of long-distance carrier confusion (Brian Holt Hawthorne)
- Intolerance and human differences (Rob Horn)
- <u>Re: Bug or Fraud (A. Padgett Peterson)</u>
- <u>Re: Voting (Karen Frenkel)</u>
- 1993 Research in Security & Privacy, Call for Papers (Teresa Lunt)

#### Issue 74 (20 August 1992)

- California Woman Convicted in Computerized Income Tax Refund Scheme (Nigel Allen)
- High-tech, discriminatory bathrooms... (Gary Friedman)
- Secret Service -- the TV show (Stephen Tihor)
- Novell Netware protection? (Fred Cohen)
- Risks of Relying on Computerized Records in Court (Mark Rasch)
- Barclays Voice-Mail system reveals card numbers (Adrian Howard)
- Voting machine failure reveals lack of backup plan (John Long)
- Macs becoming popular in Bulgaria (Klaus Brunnstein)
- Gold Card with wrong name, odd riders (Jane Beckman)
- PRIVACY Forum reminder (Lauren Weinstein)
- Issue 75 (20 August 1992)
  - CPSR Letter on Crypto Policy (Marc Rotenberg via Dave Banisar)
- Issue 76 (27 August 1992)
  - Nuclear power plant shut down (again), by walkie-talkie interference? (S A McConnell)
  - Software produces legally inadmissible reports (Les Hatton)
  - More legal stuff: CCTA, SD-Scicon, 5.5m pounds lost (Les Hatton)
  - Scientists cry foul over NASA security raid at Ames (Michelle Levander via Eugene N. Miya)
  - Unix servers and DOS viruses (Fred Cohen)
  - Re: Barclays [Hamburg] Credit Service (Klaus Brunnstein [2])
  - Re: Barclays Voice-Mail system reveals card numbers (L. Indaleci)
  - Patriot missile bug (James B. Shearer)
  - IEEE Spectrum August 1992 issue on Data Security (Olivier M.J. Crepin-Leblond)
  - Geography in 1992? Internet Course (Bob Frankston)
- Issue 77 (2 September 1992)
  - Malfunction in a collision-avoidance system (Steve Bellovin)
  - <u>Software bug on TOPEX spacecraft (sci.space.news via John Rushby)</u>
  - Software problems on Hubble too (Ron Baalke via John Rushby)
  - The endless bridge, NJ (George Sicherman)
  - Washington State felony charges for computer misuse (PGN)
  - Making a Statement (financial) (Don Grimes)
  - Feds seek customer records on "Grow-lamps" (Dan Veditz)
  - Spontaneous appliance operation (Phil Karn)
- Issue 78 (4 September 1992)
  - Re: TCAS (Nancy Leveson [2], Jim Sims)

- The Glitch Telephone Network and Janet Pensig (PGN)
- Phone Hackers (David Ashenfelter)
- 15th National Computer Security Conference, PROGRAM (Jack Holleran)

#### Issue 79 (11 September 1992)

- "Sneakers" -- A Topical Movie Review (Donn Parker)
- Police probe mans death in Citibank disk case (Pat Cain)
- <u>Arrest warrant database problems (James Hanlon)</u>
- New computer delays Berlin Fire Department (Debora Weber-Wulff)
- Hardware failure stops school (Andrew Marchant-Shapiro)
- PC board waste in San Francisco Bay (Phil Agre)
- Re: TCAS (Nancy Leveson)
- Registration and Hotel Information 15th National Computer Security Conference (Jack Holleran)

#### Issue 80 (16 September 1992)

- Arrest Warrants (Joseph Nathan Hall)
- Stop the presses, call the police! (Frans Heeman)
- A Financial risk avoided (Rob Horn)
- From the Jury Room Alcohol breath analyzer (Jim Haynes)
- Automatic DUI (Driving Under the Influence) (Jane Beckman)
- Re: update: Barclay voice mail insecurity (Flint Pellett)
- Re: "Sneakers" -- A Topical Movie Review (Mark Brader, James Zuchelli)
- Greening of Computers (Mark J. Crosbie)
- Michigan Awarded Funds to Improve Criminal History Records (Nigel Allen)

#### Issue 81 (18 September 1992)

- Bounced cheque libel (Terry Gerritsen)
- NYT reports on Smart autos; on Computer graphics at trials (John Sullivan)
- A simpler risk of computerized warrant systems (Phil Karn)
- Outstanding Warrants? (William D. Bauserman)
- More Arrest warrant database problems (Kraig R. Meyer)
- Re: Arrest Warrants (Lauren Weinstein, Randall Davis)
- Airliners playing chicken (David Wittenberg)
- Postal service privacy RISK (Daniel Burstein)
- Re: Phone numbers in popular entertainment (Sneakers) (David Paschich)
- Re: Drunk driving (Toby Gottfried, Jim Haynes)
- CPSR Files Suit Against FBI Over Wiretap Proposal (David A. Banisar)

#### Issue 82 (25 September 1992)

- Police files conference (Nigel Allen)
- Electronic mail confusion (Stewart T. Fleming)
- Duplicate Account Names (Martin Smith)
- Digitizing art (John Sullivan)
- Re: Airliners playing chicken (Rogier Wolff, Leslie J. Somos, Larry Seiler, Marc Horowitz)
- Re: Airplane chicken, scanning addresses, Sneakers (John Sullivan)
- <u>Re: Postal service privacy RISK (Kraig R. Meyer, Gene LeDuc)</u>
- <u>Re: Bounced cheque libel (Peter J. Scott)</u>
- Re: Computerized warrant systems & mobile data terminals (Michael G Kielsky)
- Re: Arrest warrants / Datamation (Lars Henrik Mathiesen, Bob Frankston, Cristobal Pedregal Martin, Geoff Kuenning)
- Issue 83 (29 September 1992)

- Computer `Kills' Prospective Jurors (Fernando Pereira)
- RISK with limited precision arithmetic (Lars-Henrik Eriksson)
- Risks of Safety Systems (Christopher Wood)
- Computer Systems Security and Privacy Advisory Board of NIST (Dave Farber)
- Therapy (Sean Matthews)
- Garage Door Openers (Mark Thorson)
- Gordon R. Dickson story "Computers Don't Argue" (Vernor Vinge, Alex Heatley, Marc Horowitz)
- Issue 84 (19 October 1992)
  - 15th National Computer Security Conference trip report (Rebecca Mercuri)
  - Vote Early, Vote Often (Bear Giles)
  - Toronto Teenager Charged in 911 Case (Nigel.Allen)
  - Rutgers students charged with scholarship scam (PGN)
  - <u>A320 engine control problem at Gatwick (John Rushby)</u>
  - <u>T\* S\* (anonymous)</u>
  - DEA mishandling of national security information (Philip R. Moyer)
  - Using the DOT's computers to steal car stereos (Bill Marshall)
  - Robot daydreaming (Les Earnest)
  - Computing Research Association (CRA) seeks assocaite (Rick Weingarten via Lance Hoffman)

#### Issue 85 (20 October 1992)

- First Day Snafu at Pittsburgh Airport (Chuck Weinstock)
- US Congress report on INSLAW case (Steve Cisler via Edward Vielmetti)
- Re: 15th National Computer Security Conference (David A Willcox)
- 6th International Computer Security & Virus Conference (Richard W. Lefkon)
- ESORICS 92: Preliminary Programme (Yves Deswarte)
- Issue 86 (24 October 1992)
  - Software Bombs Out -- Ark Royal revisited (Simon Marshall)
  - Erased Disk used against Brazilian President (Geraldo Xexeo)
  - The NSF Net cable-cut story (Steve Martin via Alan Wexelblat)
  - Risks in Banking, Translation, etc. (Paul M. Wexelblat)
  - <u>Re: 15th National Computer Security Conference (Dorothy Denning)</u>
  - Re: Vote Early, Vote Often (Louis B. Moore)
  - <u>T\*p S\*cr\*t (Berry Kercheval)</u>
  - Book Review: The Hacker Crackdown (David Barker-Plummer)
  - Filling station POS terminals: credit card users beware! (Steve Summit)
  - Int Workshop Fault and Error Models of Failures in Comp Sys (Ram Chillarege)
  - <u>Computer Security Foundations Workshop VI CFP (Catherine A. Meadows)</u>

#### Issue 87 (26 October 1992)

- US presidential election year politics help cause time zone bugs (Paul Eggert)
- Privacy of e-mail (Symantec/Borland suit) (Robert Bowdidge)
- New risk reports (Jonathan Bowen)
- The DC-10 Case (Robert Dorsett)
- Re: Erased Disk used against Brazilian President (Bob Frankston, Robert Slade)
- <u>Re: Risks in banking (Steve Lamont)</u>
- <u>T\*p S\*cr\*t II and William Safire (Bob Devine)</u>
- Conference on Computers, Security and the Law (Kimble)
- <u>Re: 15th National Computer Security Conference (A. Padgett Peterson, Peter K. Boucher, Larry Hunter, Pete</u> <u>Kaiser</u>)

#### Issue 88 (29 October 1992)

•	London Ambulance	Service	Brian Randell	, Trevor Jenkins)

- Structural Failure, Product Liability, Technical Insurance (Hermann Haertig)
- Information America (database risks) (Jan Wolitzky)
- Interesting/obscure interaction between users -- shared mem resources (David A. Honig)
- NSF Net cable-cut story is bogus (Doug Humphrey via John G. Scudder)
- Re: Risks in Banking, Translation, etc. (Arun Welch)
- Cellular reception equipment banned by Congress (Robert Allen and Mark Walsh)
- Re: Encryption keys (Dorothy Denning, Peter Wayner, Li Gong, Carl Ellison, Charles Mattair)

#### Issue 89 (2 November 1992)

- Leaving greasy marks on monitors may be dangerous (Simon Marshall)
- Risks Of Cellular Speech (Dave King, PGN)
- Police and Computers (Mark Bergman, Mike)
- Cash displenser fraud (E. Kristiansen)
- Network is a lifesaver (Mike Cepek)
- Pay-per-call-back-verify (Robert Slade)
- Re: London Ambulance Service (Brian Randell, John Jones)
- Alarmism and Prof. Denning (Timothy C. May)
- Blockbuster announces plan to use data from video rentals (John Nagle via T. Kim Nguyen)

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:

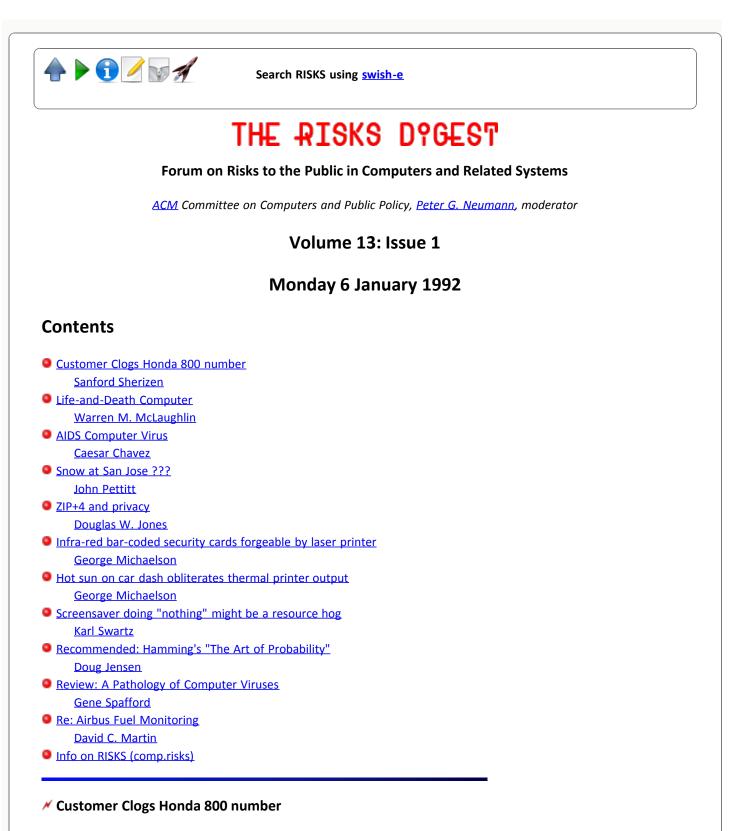
## Volume Index

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
Volume 5	<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
<u>Volume 10</u>	<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
<u>Volume 16</u>	<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
<u>Volume 19</u>	<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



Sanford Sherizen <0003965782@mcimail.com> Thu, 2 Jan 92 21:57 GMT

The Boston Globe (December 30, 1991) reported that a disgruntled Honda owner called its "Better Business Bureau Information Line" toll-free customer relations number so many times that he clogged the line. He did the same to other 800 numbers used primarily by Honda employees and dealers. In both cases, he presumably used an automatic redialing mechanism (daemon dialer). He then

began tying up a Honda facsimile number by transmitting muti-page letters during a four-day period.

American Honda Motor Co. says that it was forced to ask AT&T to step in and block the calls which allegedly came from a Holliston, Mass home. However, AT&T security said that it also had to block any calls to the Honda numbers for the entire 508 area code, which covers west and north of Boston. Attempts to reach the Holliston complainer was not possible since his phone is unlisted!

I seem to remember that a televangelist's number was tied up in a similar fashion a few years ago and there has been rumours of political candidates' phones being plugged by their competition. How common is this form of destructive behavior?

It will be interesting to see whether AT&T does some form of call or line blocking on this individual. How can phones be made open except for certain parties who overstep bounds? When are there too many calls and when is the line crossed into harassment? Is this a case where caller ID would have "proven" harassment? Under what conditions is someone no longer allowed "phone rights?" Was the Los Angeles judge's denial of telephone use by Ian Mitnick to prevent him from connecting to a computer in any way related in a legal sense to this present incident?

Good story to end 1991. The year of ousted regimes, stalled economies, and phone disorders. Sort of an updated version of Sex, Lies, and Videotapes, to be called Lex, Slides, and Telegaps.

Sanford Sherizen, Data Security Systems, Inc., Natick, MA 01760

#### ✓ Life-and-Death Computer

"Warren M. McLaughlin" <McLaughlin@DOCKMASTER.NCSC.MIL> Sun, 5 Jan 92 13:21 EST

The Washington Post, 5 Jan 1992, page C6 (the editorial page):

As technologies become more powerful, the distinction between a helping tool and a decision-making tool keeps gaining importance. Nowhere is this clearer than in the case of the new diagnosis-aiding computers, which offer doctors the benefit of a gigantic data base -- far larger than their own experience could be -- compiled from the results of many thousands of cases nationwide. By conglomerating and analyzing the results of these cases, the computer can read out a series of alternative treatments, a probability rating on the success of a given procedure or -- most controversially -- the statistical risk of a patient's dying upon arrival in an intensive care unit in a given condition. Physicians with access to such a machine now bear a responsibility at least as weighty as that of diagnosis itself: that of balancing the computer's seemingly precise numbers and instant certainties with the knowledge that its results are dependent upon human judgement.

According to the staff in a Michigan hospital using a program of this type called APACHE, the computer's predictions of a patient's statistical

probability of dying -- calculated to two decimal points -- are used strictly as tools, rather as any doctor might estimate, say, a 10 percent chance of survival from a given operation. A better description of risk, in that scenario, need not govern the doctor's (or the family's) decision as to whether the risk should be taken, only inform it better than individual experience ever can. But the incomplete results of a different study performed in France suggested that doctors with access to that kind of risk data were more likely than others to terminate care. The fear among practitioners is that hospital administrators or health bureaucrats, all increasingly beleaguered and pushed by public pressure toward cost-cutting, might see computer-confirmed statistics on death risk as a road to easier triage.

Given the capability for vastly enhanced diagnosis by means of computers, the medical profession will be stuck with the same responsibility -- also vastly enhanced -- as before: first, to recognize that a computer can serve the cause of accurate diagnosis only on the basis of properly entered information by the physician using his or her senses; second, to keep in mind a fact much of the general public has trouble with, which is that a statistic about the probability of an event bears no causal relationship to that event. A person with a 95 percent chance of dying under a procedure is not the same thing as a person whom that procedure cannot help, or a person from whom care can be withheld with no compunctions. Obscure that distinction, and you take a step toward making the computer the master -- a bad one.

- Mike

PO Box 54, Bridgewater, VA 22812-0054

#### AIDS Computer Virus

<Caesar\_Chavez.ES\_AE@xerox.com> Fri, 3 Jan 1992 04:32:47 PST

- - - - - -

Remember that "AIDS Computer Virus" that was distributed about two years ago? The following article appeared in Information Week on December 16, 1991 on page 40.

Caesar Chavez

"PC VIRUS BLACKMAIL

"A bizarre British court case involving computer viruses has pointed up the vulnerability of users with careless policies on PC software.

"Hearing the case of a U.S. scientist accused of computer blackmail late last month, the court granted a stay after lawyers successfully argued that the defendant, Joseph Popp, 41, was mentally ill. Popp was facing 11 charges of damaging computer systems and attempting to obtain a total of 6 million pounds (\$10.7 million) through blackmailing numerous medical institutes worldwide around Christmas 1989.

"Popp is alleged to have mailed more than 20,000 floppy disks to the research institutes. He promoted the disks as containing valuable information about AIDS. But the disks themselves contained a software virus, which has since

also been dubbed AIDS. When users tried to access the disk, they got messages demanding 200 pounds (about \$350) to eradicate the virus that had just infected their systems.

"Popp was extradited to the United Kingdom, where a chorus of scientists from universities and research institutes claimed that their software had been damaged when the disks were loaded onto their systems.

"One organization that fell foul of the virus was the Imperial Cancer Research Fund in London. Dr. Ron Catterall, director of the fund's computer research unit, was called as a witness for the prosecution. Catterall was smart: He loaded the disk onto his standalone PC rather than the network, and warned other users as he discovered the virus. `It took a long time to find out what was going on, and to clean up my machine,' he said. `It eventually started overwriting the hard disk.'

Philip Hunter."

#### Snow at San Jose ???

John Pettitt <jpp@slxinc.specialix.com> Tue, 31 Dec 91 09:54:53 PST

The FAA has an on line pilot briefing sysem called DUAT (Direct User Access Terminal). The version of the service I use is provided by Contel Federal Systems. For those who are not familiar with aviation weather the raw data is supplied in a very cryptic form. To make simplify things for users DUAT has a decoder that expands this into `english'.

However last night the FT (Terminal Forecast - a 24 hour forward forecast) for both San Jose (SJC) and San Francisco (SFO) was showing 3 VBSY which was being decoded as:

Visibility 3 in snow and blowing spray

There seem to be two possible causes:

a decode error (I don't know what the correct decode of VBSY is)
 VBSY does mean snow and spray and the NWS screwed up the forecast.

Either way computer weather briefing has a way to go yet.

John Pettitt, Specialix International (jpp%slxinc@uunet.uu.net)

[In response to my comment that Mt Hamilton is east of San Jose and Mt Diablo east of Oakland, and they do get snow now and then, John noted that the terminal forecast is for conditions on the airport and within the Airport Traffic Area (ATA), which is 5 miles radius. <"Anyway, I called the DUAT help desk and they thought the idea of snow was rather a good joke - `another bug for the list'." (John)> PGN]

ZIP+4 and privacy

Douglas W. Jones,201H MLH,3193350740 <jones@pyrite.cs.uiowa.edu> 2 Jan 92 22:58:44 GMT

I recently asked at my post office how many houses shared the same ZIP+4 code with my house. The answer was that if I lived in a single-family dwelling, I almost certainly have a unique ZIP+4 code.

I note that the USPS now provides a complete database of ZIP+4 addresses in the country -- it is on CDROM, and it is included in the postal exhibit in Chicago's Museum of Science and Industry, where you can type in your address (as you would on a letter), and it gives you your ZIP+4 in response. I tried it on my address here in Iowa, and it worked correctly.

The risk I see in this is that statistical data that has traditionally been available sorted by ZIPcode (for example, census data) may be released broken down by ZIP+4 codes. If this is done, it destroys any promise of confidentiality for such data.

Of course, there is a benefit -- you should be able to send mail to me with only a ZIP+4; no need to mention city, state, street, or house number.

Doug Jones

## infra-red bar-coded security cards forgeable by laser printer

George Michaelson <G.Michaelson@cc.uq.oz.au> Sat, 4 Jan 1992 12:54:31 +1100

They handed the cards out in alphabetical order to staff, and the barcodes/card numbers were congruent and the batch was sorted. Skilled person (not self) examined 3 in sequence, calculated trivial encryption and checksum algorithm used, inferred card for senior member of staff, used Public Domain code to generate barcode strip on apple laserwriter, glued to card and swiped through lock. bingo! instant access to secured areas, leaving calling card of selfsame high-up all over the online logs.

Infra-Red readers also handle normal light codes. Good eyes can read thick/thin sequences in strong light so even if numeric code on card doesn't match bars, its forgeable. Infra-Red also pretty trivial to obtain as it UV reader.

I really think the local admin/security people have been blinded by science. Apart from anything else the electromagnets which operate the doorlocks look very subvertable. Another instance of hindering the novice and legitimate, whilst barely impeding anybody intent on skullduggery.

-George

## **\*** Hot sun on car dash obliterates thermal printer output.

George Michaelson <G.Michaelson@cc.uq.oz.au> Sat, 4 Jan 1992 12:47:55 +1100 Buy parking ticket @ 40c per hour. Vending machine has current TOD, allocates ticket to nearest 20 minutes to be displayed clearly on dashboard of parked car. Shows purchase time, and expiry time in large letters.

Come back to car 7 hours later. It has been a hot muggy day, around 35C at the peak. Car was parked in full sunlight, and is dark (rusty!) brown. Interior could well have been 40C or over. (certainly felt sauna-ish inside)

Entire parking voucher is black. Either the spot heat, the continual lower background heat, some emitted vapour from the car interior, or all three has made it do a disappearing fax trick in reverse. Illegible unless scrutinized at close range, certainly not readable through window.

I hope nobody's using one of these to do "permanent" chart recording or whatever in hot locations...

-George

#### Screensaver doing "nothing" might be a resource hog

Karl Swartz <kls@ditka.chicago.com> Fri, 3 Jan 92 0:07:51 PST

This afternoon, a colleague at SLAC (the Stanford Linear Accelerator Center) was showing me the latest screen lock and saver program he had obtained for his workstation, a port of the one often found on Suns. This reminded me of an incident several years ago when I was visiting my friend George Berg.

George is a professor of computer science at SUNY Albany, known in the department for his AI programs that run for days or even weeks at a time on several SPARCstations, grabbing every available CPU cycle. Over the weekend, George dialed in from home to check on the progress of his latest project and was a bit surprised to find that it seemed to be running much more slowly than it had during the week. When a later checkup again showed minimal progress he began to invistigate, and found that the machine was indeed busy -- running Life on the unused screen in his office! After disabling the screen saver the real work continued on without further competition.

Getting back to SLAC today, this is quite relevent as some of our computing tasks involve many essentially unrelated events, work that can easily be farmed out to machines on the network with cycles to spare. Obviously productive use of our resources depends on users understanding that "their" machine isn't necessarily free to simulate life, compute pi to a million decimal places, or enumerate the nine billion names of God just because they aren't in the office. It's also easy to forget just how many resources some "cute" program can use.

Karl Swartz uunet!decwrl!ditka!kls 1-415/854-3409 2144 Sand Hill Rd., Menlo Park CA 94025

#### \* Recommended: Hamming's "The Art of Probability"

"DOUG JENSEN, DTN 223-1201, M.S. PKO3-1/22D" <jensen@helix.enet.dec.com> Wed, 1 Jan 92 17:45:56 PST

I have recently been reading Richard Hamming's book "The Art of Probability," (Addison Wesley, 1991) and wish to strongly commend it to those of you who haven't yet seen it. Please allow me to whet your appetite with the following brief excerpts.

"This book...is one man's opinion using a rather more scientific (as opposed to mathematical) approach to probability than is usual."

"Most authors of probability books present one version of probability as if it were the true and only one. On the contrary, we have carefully developed a sequence of models on what seems to be a reasonably scientific approach."

"The model of probability you adopt is often relevant to what actions you later take, though most statistics books do not make plain and clear just what is being assumed. Unfortunately, many times the statistical decisions affect our lives, from health, medicine, pollution, etc. to reliability of power plants, safety belts vs. air bags, space flights, etc."

"The weak law of large numbers encourages one to think that the average of many repetitions will give an estimate of the underlying probability. But we have seen...that the number of trials necessary to give an accurate estimate of the probability may be much more than we can ever hope to carry out. And there are further difficulties. We assumed the existence of the mean; suppose it does not exist! (see the next Section 8.7). It is not that the author is opposed to statistics--there is often nothing else to try in a given situation--but the stated reliabilities that statisticians announce are often not realized in practice. Unfortunately, the foundations of statistics, and its applicability in many of the situations in which it is used, leaves much to be desired, especially as statistics will probably play an increasingly important role in our society."

## Keview: A Pathology of Computer Viruses

Gene Spafford <spaf@cs.purdue.edu> 31 Dec 91 23:09:21 GMT

I recently received a copy of "A Pathology of Computer Viruses" by David Ferbrache of the UK Defense Research Agency. The book is copyrighted 1992, and is published by Springer-Verlag (ISBN 3-540-19610-2 and 0-387-19610-2). US price was \$39.50. 300 pages.

This book is an extraordinarily comprehensive book on the history, theory, and operation of computer viruses, and on virus countermeasures. It is the most complete book I have seen on the topic to date, and contains a very detailed description of how PC viruses work and spread, including viruses in networked environments, viruses in Amiga systems, and viruses in Unix. In fact, I expect David to get some criticism for the detail he presents, but it serves to make the subject matter much clearer.

Chapter 1 is a general introduction to the topic of viruses, worms, and malware. Chapter 2 is devoted to the history of viruses and "malware" starting from the 1960s and thru the end of 1990. It has a very complete description of the earliest viruses, including some events and activities that have not been generally reported elsewhere. It also includes interesting information on related activities, such as the founding of the Virus-L mailing list.

Chapter 3 is a nice introduction to the theory of computer viruses, including discussion of how computer viruses relate to biological viruses, and other related topics such as artificial life.

Chapter 4 is a detailed discussion of how viruses operate in an IBM PC environment. This includes details on camouflage techniques and signatures as well as spread and activation. Chapter 5 provides extensive discussion of techniques to protect against computer viruses. Chapter 6 is a description of how viruses work in the Apple Macintosh. Chapter 7 discusses viruses in mainframes and Unix systems.

Chapter 8 is devoted to "network viruses" -- worms. This includes analysis of early work, the Morris Worm, WANK, Christma Exec, and even a discussion of e-mail chain letters! The chapter also has a nice discussion of Internet protocols that lend themselves to abuse by malicious code.

Chapter 9 is a chapter discussing reactions of the computing community, including some legislative history and information on the formation of response teams. Chapter 10 is a brief statement about the future of the problem.

The book concludes with 18 appendices, listing everything from the DOS filestore structure to a PC virus family tree to all the CERT advisories to date. One of the appendices provides an extensive reading list.

Overall, the book is one of the best books on computer viruses I've seen. David's illustrations are clear and his prose is quite readable. I found information and details in this book that I have not seen in any other virus book. The section on the history of computer viruses, in particular, is quite well done.

There are some small problems with the book, however. First of all, I was very disappointed that there were almost no footnotes or citations in the body of the book. As I read through the material I noted material that I wished to pursue further -- unfortunately, there were no citations to allow me to seek original sources. I do not doubt the accuracy of the information presented, but I feel that the lack of specific citations is a flaw in such a scholarly work.

The book suffered from spotty copy-editing. I found many places where there were quite obvious typos. In a few places, these typos obscured the text's meaning or distorted some information. I am not sure whether to fault the author or the publisher, but is is sad to see in an otherwise excellent book by an established publisher.

Another minor complaint is that there is no presentation of formal theory about viruses or worms. Although this is not an area that has seen much good work,

it would have been useful to have some coverage of that material here to complement the higher-level descriptions.

The appendix listing other references was good, and contained some references I have not seen before, but it did not give any indication which of the many references were particularly noteworthy or why the references were cited. For instance, a number of limited-availability BBS postings and Usenet articles were cited without an indication of why they were included. At the same time, the references did not list either of the fine collections of readings by Professor Peter Denning ("Computers Under Attack" ACM Press/Addison Wesley) and Professor Lance Hoffman ("Rogue Programs" Van Nostrand Reinhold), nor did it reference any of the publications by the NCSA.

The book is written primarily for a British audience. This means that the coverage of US-specific items, such as anti-virus legislation, is briefer than a US reader might prefer. It also means that some small translation of terms is necessary in spots; of course, this same criticism can be made of many US-centric books being published in a non-US market.

Despite these criticisms, I strongly recommend this book to anyone who is interested in computer viruses and security. It presents material clearly and comprehensively, and provides unbiased coverage of the area (David is not involved with the marketing of anti-virus software or seminars as are many other virus book authors).

#### (317) 494-7825

Gene Spafford, NSF/Purdue/U of Florida Software Engineering Research Center, Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-1398

#### Ke: Airbus Fuel Monitoring (Van Voorhis, <u>RISKS-12.72</u>)

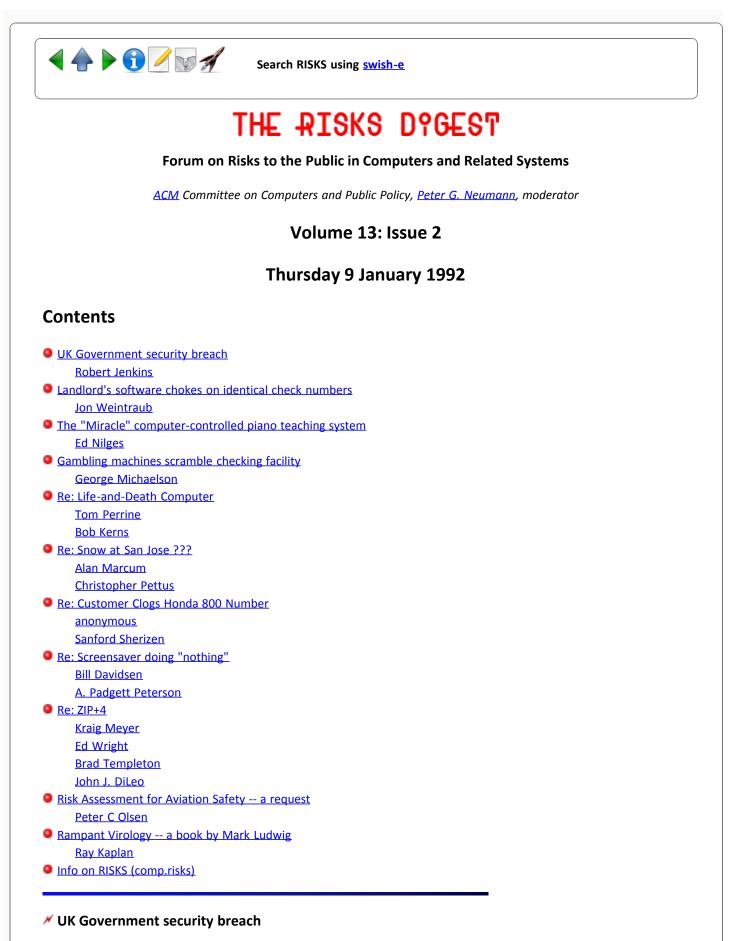
David C. Martin <owner-comp-sources-x@msi.com> Tue, 31 Dec 91 07:32:25 PST

Fueling is performed by an external source, not by the plane (at least for all the American made planes that I have worked with, e.g. MD-80's, 727's, etc..) The plane has a control panel which works on conjunction with the fueling system from the tanker to indicate how much fuel the plane should take (i.e. how much do you want to put in) and then automatically cuts off the flow when either the limit of storage or the limit of input has been reached. There are internal pumps to move the fuel around from tank to tank.

It sounds like the fueling panel on the plane was not working correctly and they needed to manually determine the amount to input. This is typically done my either disabling the fueling panel (or overriding the auto-cutoff) and determining the fueling progress from inside the cockpit. One problem with this technique is that it requires multiple people (one in the cockpit, one at the pumping station, and maybe others from the airline to supervise the override/disable of the fueling panel).

This practice is quite common w/ older American jets and only occasionally causes problems, e.g. when fuel spills due to other malfunctions.





Robert Jenkins <rjenkins@cix.compulink.co.uk>

Wed, 8 Jan 92 20:52 GMT

The Guardian of 8 January carries the following report, headlined "Security Flaw in Whitehall":

Fake names were fed into a Whitehall [i.e., central government] computer to give unauthorised staff access to details of top security safes holding cabinet papers and sensitive defence documents, an investigation by the National Audit Office, parliament's financial watchdog revealed yesterday.

The issue of security furniture, such as filing cabinets for classified documents, was "left in the hands of an inexperienced officer who had virtually unlimited control of the system and was not effectively supervised," says the report.

It goes on: "Control over access to the computer system was minimal; staff who were no longer authorised to use it, and two fictitious names thought to have been entered by a previous employee, continued to have access.

"Staff training was inadequate, procedures were not documented, and inaccurate stock information was leading to the posting of wrong figures to the accounts. The staff were unable to generate invoices for equipment and substantial amounts had consequently not been charged. At least one duplicate payment, amounting to 92,000 pounds, had been made to a supplier."

The report said there was no evidence of fraud, "but the serious lack of control, and the limited audit trails, made it impossible to provide an unconditional assurance that it had not."

#### ✓ Landlord's software chokes on identical check numbers

Jon Weintraub <weintrau@earth.eecs.uic.edu> Thu, 9 Jan 92 12:48:53 -0600

My landlord has been `politely threatening' us since the first of the year for overdue rent. After careful checking, the problem was that both my roommate and I each happened to pay with a check numbered 144 from our respective accounts. The computer supplanted its record of the first check with its record of the second -- it was counting on check serial number to be a unique identifier across accounts! If we were less lucky, we might be in court over this by now.

#### \* The "Miracle" computer-controlled piano teaching system

<EGNILGES@pucc.Princeton.EDU> Tue, 7 Jan 1992 17:11:16 GMT

This morning (7 Jan 1992) on the Today show, the "Miracle" computer-controlled piano teaching system from the Software Toolworks was demonstrated for announcer Katy Couric. This is a high-quality electronic piano and software running on several platforms (including the Mac and the PC) which teaches piano by lessons and by monitoring play on a key-by-key basis. It was the subject of some reasonably smarmy ads as Yuppie parents watched, eyes glistening, as their Little Darlings played rather complicated pieces reasonably well. The performance in the ads has been borne-out by tests of the system; it is a good way of teaching piano skills, interpreted as being able to play the music on the page. Thereby, however, lies a potential Risk to music aesthetics.

For when Katy Couric played a decent version of "Happy Birthday", including some rather elegant grace notes, the computer gave her a low score of 38%. This is it could not recognize the slight improvisation represented by grace notes as an improvement over the music displayed on the screen. In my opinion, a good piano teacher would give Couric a higher score for the creativity implicit in grace notes.

More than this, the developers of "The Miracle" seem unaware of the fact that Playing The Music Exactly As Written (PTMEAW) is (in a global sense) not the usual practice. Not only is folk music almost completely improvised, Indian classical music gains much of its richness from being IN PART improvised by master musicians every time it is performed. Even in the Western classical tradition, improvisation was the norm prior to the Baroque era. Deliberate error, even, has played an extensive part in music. Italian and German violinists of the 17th century used a system of deliberately "incorrect" tuning, called "scordatura", by which the Baroque composer Biber gained much emotional intensity in his violin sonatas. Up until Beethoven the instrumentalist in a concerto provided a "coda" in which the soloist could improvise on the theme, so PTMEAW was not even the norm in Mozart's time.

Nowadays, although classical music is subject to PTMEAW (with the absurd stress on "original instruments" being part of this), non- classical music, including folk, rock and country gains much of its liveliness by retaining both improvisation and "scordatura" (that is, deliberate error for emotional intensity.)

"The Miracle" completely ignores this by assigning high scores in a dehumanized fashion to students who, unlike Couric, don't have the creativity to improvise. I predict that two types of populations will evolve on "The Miracle": unimaginative keyboarders of the music as written, and hackers, who will misuse the features. In neither group will true musicians be found.

"The Miracle" does look like a useful tool for learning music, but I object both to its operatic name, which makes an overlarge claim, and to its incorporation of numeric scoring. The designers could have (under the advice of a decent musicologist) deliberately eschewed the assignment of numeric scores and restricted themselves to the display of natural-language evaluations.

#### ✓ Gambling machines scramble checking facility

George Michaelson <G.Michaelson@cc.uq.oz.au> Tue, 7 Jan 1992 10:02:53 +1100

ABC Radio (Australia) reported this morning that different manufacturers "one

armed bandits" (in-line gambling machines) confuse the centralized checking systems to which they are networked, and destroy each others records.

This has delayed installation of the systems in clubs and hotels around the state of Queensland, until new code can be put in to ensure they can be checked up on.

Worry about abuses of the machines for gambling, tax evasion and links with crime (for money laundering, and alleged mafia involvement in the manufacture & distribution) has been a big political football here. -George

#### Ke: Life-and-Death Computer

<tep@tots.logicon.com> Tue, 7 Jan 92 11:03:13 PST

The Washington Post editorial in <u>Risks 13.01</u> (Subject: Life-and-Death Computer) overlooked one other problem with the APACHE software: it has the potential to generate self-fulfilling prophecies.

It appears that APACHE is really reporting on patient "profiles": age, weight, general medical condition, cross-referenced with specific complaints or injuries and treatments and survival rates.

Since APACHE reduces people to profiles, we might as well use that term in discussion.

Lets say that a "profile" is not treated with a given procedure, in part due to the "advice" of APACHE, and then dies. If the information concerning this "profile" is then fed back into the APACHE database, this will decrease the "survivability" quotient for subsequent "profiles" with the same initial set of problems. Each time a patient (oops, "profile") with a given complaint is not treated (and dies), the survival quotient decreases again.

Each time APACHE (indirectly) advises a doctor to withhold treatment for a condition, it increases the probability that it will "advise" withholding treatment for the next patient (oops, "profile") with the same basic complaint/injury, leading to another death, leading to another survival quotient decrease.

The editorial remarks that "a computer can serve the cause of accurate diagnosis only on the basis of properly entered information by the physician using his or her senses". Even if data is 100% correct, it still leads to positive feedback which will further skew the output data.

Tom Perrine (tep), Logicon - T&TSD, P.O. Box 85158, San Diego CA 92138 +1 619 597 7221 UUCP: sun!suntan!tots!tep

#### ✓ Life-and-death computer: Numbers lie

<rwk@crl.dec.com> Wed, 8 Jan 92 06:12:15 -0500

In <u>RISKS 13.01</u>, Warren McLaughlin cites a Washington Post article about programs which give highly-precise probabilities on medical treatment outcomes, and how this can lead to doctors relinquishing their proper decision-making responsibility.

It seems clear to me that the problem here isn't that the doctor is relinquishing his responsibility by being too trusting of the software, so much as it is the programmer is relinquishing the responsibility to the doctor by presenting bad information.

The problems inherent in encoding weights for different courses of action (or any other "non-monotonic" comparison) is very familiar to anyone familiar with expert systems. In addition to the illusion of accuracy illustrated in the article, there are numerous other kinds of error introduced at every step, from the initial assignment of weights for the raw data (what is a "favorable outcome" in treatments to prolong life in a terminal disease), observed situation (what is "slight swelling of the lymph nodes"), anomolies when these are reasoned on in conjunction with each other (often you can prove a>b>c>a), and then, finally, in the way they are reported.

Assuming that these problems are dealt with in a realistic manner, for the program to communicate reasonably with the doctor, it is necessary to give some idea of the precision of these numbers. One of the better techniques is to use "error-bars". This can help transform what appears to be a definitive decision:

Cut off head: 40% Give aspirin: 30% Cut off foot: 20%

vs:

-Treatment- 0 10 20 30 40 50 60 70 80 90 100 Cut off head: |-----X----| Give aspirin: |----X-----| Cut off foot: |---X------|

As you can see, this makes it much more clear that the program really hasn't decided much of anything at all.

It should also be clear from my example that in addition to the numerical information, an explanation of the reasoning process together may well be warranted, to check for any unwarranted assumptions, and other things to look out for. (Such as the need for reattaching the head after repairs are effected, and the assumption that the patient is a robot).

(The disease in question, of course, is "headache").

In real life, a doctor giving a second opinion isn't just going to give a number. He's going to give reasons, and an idea how sure he is of the appropriateness of a particular treatment and alternative treatments and even perhaps alternative diagnosis to consider. [Or maybe the insurance industry has this process reduced to a coded number now too, in which case, the Risks should be obvious].

The deceptive problems of encoding preferences and subjective evaluations into numbers is, of course, a pervasive problem in other areas. Indeed, the entire area of risk analysis is rife with it, as I've pointed out indirectly in other messages. It's so much easier to calculate with simple numbers that this is a very tempting trap to fall into. But we must resist the temptation to manufacture certainty where non exists. Whether we are computer professionals, scientists, pollsters, or journalists, or newspaper reader I think being careful with these issues is a matter of professional integrety. It's an integrety which is all too often lacking, out of ignorance, sloppiness, desire to persuade, or desire to be persuaded.

[finger rwk@... suggests this might be someone named Bob Kerns. PGN]

#### Ke: Snow at San Jose ??? (Pettitt, <u>RISKS-13.01</u>)

Alan M. Marcum - Tech Support <Alan\_Marcum@NeXT.COM> Mon, 6 Jan 92 14:47:46 PST

> 1) a decode error (I don't know what the correct decode of VBSY is)> 2) VBSY does mean snow and spray and the NWS screwed up the forecast.

There's a third possible cause, which I guess I'd call the probably cause. Someone made a typographical error. VSBY is the contraction for visibility. BSY could well translate to snow and blowing spray.

For the RISKS folks, note also that the translation Contel provides is made available as a courtesy. They have a large disclaimer stating this, and requesting that the pilot acknowledges his responsibility for correct translation according to the relevant portions of the Federal Aviation Regulations.

There is the RISK, though, of typos in critical information with little or no redundancy, such as the FAA's cryptic weather information.

Alan M. Marcum, NeXTedge Technical Support, amm@NeXT.COM

### Ke: Snow in San Jose ??? (<u>RISKS-13.01</u>)

Christopher Pettus <cep@Apple.COM> 6 Jan 92 21:57:25 GMT

>Either way computer weather briefing has a way to go yet.

Indeed. One of the problems with computerized decoding of National Weather Service (NWS) weather information is that the format, while supposedly standardized, is actually typed in by humans with no checking in a pretty free-form format. In this case, the answer is both (1) and (2). A terminal forecast has two parts, an 18-hour "forecast" and a 6-hour "categorical outlook" (although even weather briefers are often unaware of the difference). The forecast is relatively detailed: the clouds are going to be at 4000 feet, it's going to be raining, the visibility is going to be 5 miles in fog, etc.

The categorical outlook is pretty generic, and just makes braod claims about the weather, in particular ceilings greater than 3000', visibility greater than 6 miles, etc. If the visibility is expected to be restricted, "VSBY" is put into the categorical.

In this case, the forecaster expected the visibility to be at three miles, so he stuck a 3 in the categorical (free-format, no checking). This is not a meaningless thing to do, since three miles of visibility is a "magic number" (it allows flight operations that might otherwise be prohibited).

This isn't what the "official" format allows, so the program decided that it had just hit a standard notation for visibility, where the visibility is given in miles, then followed by letter codes for what kind of goo is restricting the visibility (for example, "2RF" means "visibility 2 miles in rain and fog"). "S" is snow, "Y" is spray, and "B" in front of a code means "blowing," and the "V" I assume was ignored, so we have "Visibility 3 miles in snow and blowing spray."

The whole weather reporting system is based on ancient 110-baud teletype technology, and is in desperate need of being trashed and redone. But it probably will not be for many years.

-- Christophe

### Ke: Customer Clogs Honda 800 Number

<[anonymous]> Mon, 6 Jan 92 22:06:51 PST

It is pretty well established that such abuse of an 800 number (or any number for that matter) constitutes harrassment. In the famous case of the guy doing this to the tele-evangelist, I believe that the caller was prosecuted, found guilty, and had to make some sort of restitution.

Keep in mind that virtually all 800 (and 900) customers already receive the caller's number for about 95%+ callers via the carriers' Automatic Number Identification (ANI) systems (this is actually different from Caller-ID, but the distinction is too complex to elaborate on here). Only larger customers usually receive this information in real-time with the call, but most receive the caller numbers with their phone bills, or sometime after the call via other means, and abusive patterns can be clearly seen in such data.

### ✓ Customer Clogs Honda 800 Number (Cont.)

Sanford Sherizen <0003965782@mcimail.com> Wed, 8 Jan 92 01:54 GMT

There is more about this incident. According to the TAB, a very good local newspaper in this area, Daniel Gregory has been charged with telephone harassment after he made at least 100 phone calls in one day and faxed a 14-foot computer banner saying "Dan Gregory is unhappy with his Honda." Gregory admitted making the calls. "It could have been as many as 100 in one day," he said last week. "MAYBE I OVERDID IT. BUT EVEN IF THAT WAS THE CASE, SO LA DE DA." (Emphasis added by me to highlight why the U.S. is in decline)

He made a comment about the long fax. "A roll of fax paper is \$12 at Staples (office store). We're talking about a multi-million dollar company getting mad because I use a lot of fax paper?"

While this story has received some coverage around the U.S., it has been treated as if it is a funny story. Some form of man-bites-Honda. The fact is, however, that this incident shows a vulnerability of technology. Is this phone clogging almost a virus-type phenomenon? Can it be possible on a larger scale? Say someone doesn't like their boss, the Internal Revenue, their ex-spouse, a political candidate, a computer network, or some other party. Then "la-de-da" is the right response.

For all we know, Gregory may run for national office on the La De Da Platform. Oop, sorry, I think that political platform is already taken by at least one other candidate for president.

Sanford Sherizen, Data Security Systems, Inc., Natick, MA 01760 USA

### Ke: Screensaver doing "nothing" might be a resource hog

bill davidsen <davidsen@crdos1.crd.ge.com> Wed, 8 Jan 92 09:12:47 EST

Also note that "screensavers" and "lock screen" programs can use a lot of ethernet bandwidth if you run them on X terminals. This can actually be enough of a factor to measure, particularly if you have a site where people tend to lock a lot of terminals at night while the administration is trying to take dumps over the net.

bill davidsen (davidsen@crdos1.crd.GE.COM -or- uunet!crdgw1!crdos1!davidsen)GE Corp R&D CenterModerator comp.binaries.ibm.pc and 386-users digest.

#### ScreenSavers & Resource Hogs (Swartz, <u>RISKS-13.01</u>)

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com> Tue, 7 Jan 92 09:28:30 -0500

The comments concerning the effects of a screensaver on a Sun station brings to mind a couple of incidents that occured a few years ago on our Vax systems.

The first involved a brand new, state-of-the-art VAX 11/780 and a digital "clock" (with alarm). A short (50 or 60 lines) DCL program, it was quite popular until it was found that four simultaneous "clocks" would swamp the 1 VUP 780 and cause logins to take upwards of five minutes.

The second was a program that used QIO and QIOW calls (never could get all of the commas straight without help) that enabled the VAX to function as a terminal emulator. Add in a Racal-Vadic 1200 baud (great improvement over 300 baud Silent 700s) modem and it was possible to debug systems in New York from my desk in Florida. With a TekHex conversion, binary traffic was also possible (this was before XMODEM, KERMIT, or UUENCODE programs were available so everything was "home grown" but worked) so we could make "on-line" fixes to a Mil-Std-1750A program.

Trouble was that in order to make a multitasking system operate as a terminal, constant cyclic checking of the workstation port and the output port was necessary. As a result the program was something of a hog and we were politely requested to only use it when necessary, preferably after hours.

In any event, one Friday an engineer left work with his terminal still running the program (this was a \*long\* time ago) even though the phone was hung up. Three weeks later we got the bill for that weekend from the computing center: \$32,000.00 for resources used. Needles to say some frantic negotiations ensued.

Of course the high cost of VAX time back then is what financed the PC revolution here so it wasn't all bad, just "there is nothing new under the Sun" (sorry).

### Re: ZIP+4 (<u>RISKS-13.01</u>)

<kmeyer@aero.org> Mon, 06 Jan 92 15:38:39 PST

jones@pyrite.cs.uiowa.edu (Douglas W. Jones,201H MLH,3193350740) writes: >I recently asked at my post office how many houses shared the same ZIP+4 code >with my house. The answer was that if I lived in a single-family dwelling, I >almost certainly have a unique ZIP+4 code.

[Unique ZIP+4] was not the intended or actual implementation of ZIP+4 that I'm familiar with. Generally, the last 4 digits indicate which block the address lies in (or sometimes additionally, which side of the block). My parents live in a subdivision in Michigan with one acre lots, and they share their ZIP+4 code with 1/2 miles' worth of single family dwellings, because that is the distance between the two cross streets. The other side of the street has a different ZIP+4 code, even though all of the mailboxes are on the same side of the street.

Check out a ZIP+4 directory at your local post office to see who you share your ZIP with.

Kraig R. Meyer

[Also noted by the following:

johnl@iecc.cambridge.ma.us (John R. Levine) merlyn@iwarp.intel.com (Randal L. Schwartz) seidel@puma.sri.com (Craig Seidel) brock@cs.unca.edu (J. Dean Brock) goldsten@m.cs.uiuc.edu (Arthur Goldstein) sullivan@geom.umn.edu (John Sullivan) and PGN himself, who owns a ZIP+4 that is unique -- which is the case for box numbers in small post offices. PGN]

#### Re: ZIP+4 (<u>RISKS-13.01</u>)

Ed Wright <edw@sequent.com> Thu, 9 Jan 92 10:21:53 PDT

The Zip + 4 system gets your letter to the correct carrier, correct side of the street, correct two block segment.

Soon Zip + 6 will emerge (its under test now) and that will give each address a unique numeric sequence.

#### Re: ZIP+4 (<u>RISKS-13.01</u>)

Brad Templeton <brad@looking.clarinet.com> Tue, 7 Jan 92 20:26:22 PST

Actually, rather than letting people mail to me with my Zip+4 (which only specifies some people exactly and not others) I would rather the post office (and other shippers) implement a scheme where I can get a unique code (number or alpha), perhaps of my choice, which identifies my address in Post Office computers, and only there.

People would be able to mail to: Code: foobazbarx, U.S.A.

And the mail would get to me. The P.O. would be pledged never to reveal where I actually live except on court order. In fact, the actual information should only be available in the local post office computer -- other computers would only know which local post office to send mail for foobazbarx.

Naturally, you could have more than one code, if you wish to pay. Mailers would be free to add more redundant information, but you would want a check letter (the x) on the end so that people who take down your address can be sure they have it right when they are talking to you.

There's a real way to use computers to preserve your privacy, and make mailing and address transcription easier, too.

#### Re: ZIP + 4 codes

"John J. DiLeo" <dileo@amsaa-cleo.brl.mil>

9 Jan 92 23:56:16 GMT

... For the more stout-hearted (and those to whom the CD-ROM is not available), all government depository libraries should have a full set of printed directories (I filed them in the depository stacks at Johns Hopkins when I was a student employee there). Entries are listed by: 1)City name/Post Office name; 2) Street name/P.O. Box group; and 3) numerically by block numbers.

John DiLeo, dileo@brl.mil

#### Kisk Assessment for Aviation Safety

Peter C Olsen <pcolsen@super.super.org> Wed, 8 Jan 1992 02:30:30 GMT

I'm doing a strategic study on aviation security and I'm looking for information about techniques that might be used to model the threat, risk, and effectiveness of countermeasures in commercial aviation security ---particularly airline security. I am particularly interested in approaches that might be useful in helping to quantify and refine the qualitative data which seems to be all that is available. Similar problems have been addressed by the people in the computer security and nuclear safety arenas.

I'd appreciate any information or advice.

Please reply to ME via email because I don't follow this newsgroup; I will summarize if there is any interest.

Peter Olsen

pcolsen@super.super.org ..uunet!super!pcolsen PO Box 410, Simpsonville, MD 21150 202-366-6525 (office)

#### 🗡 Rampant Virology

Making memories <KAPLAN@ccit.arizona.edu> Wed, 8 Jan 92 20:51 MST

More books to keep you awake at night (I've only seen volume 1 so far.)

The Little Black Book of Computer Viruses, 169 pages, Mark Ludwig, ISBN 0-929408-02-0, \$14.95 - American Eagle Publications, P.O. Box 41401, Tucson, AZ 85717 - (602) 888-4957. (Thanks to Winn Schwartau for this referal to a publisher right here in my own town!)

The back cover of this one tells it all:

WARNING. This book contains complete source code for live computer viruses which could be EXTREEMELY DANGEROUS in the hands of incompetent persons. You can be held legally liable for the misuse of these viruses, EVEN IF SUCH MISUSE IS UNINTENTIONAL. Do not attempt to execute any of the code in this book unless you are well versed in systems programming for personal computers, and you are working on an isolated machine.

Introduction: "This is the first in a series of three books about computer viruses... All three volumes are full of source code... It is enevitable that these books will offend some people ... The first volume is a technical introduction... The second volume discusses scientific applications... The third volume discusses military applications ... (And, a lengthy disertation on everything from the social meaning of this all to the "why do it" of it all (that would play very nicely here in RISKS.?))

```
Vol 1
```

- Ch 1 The basics Types **Functional elements** Tools needed to write viruses
- Ch 2 Simple COM file infector
- Ch 3 Sophisticated executable virus
- Ch 4 Simple boot sector virus
- Ch 5 Sophisticated boot sector virus
- Appendix 1 TIMID
- Appendix 2 INTRUDER
- Appendix 3 A basic boot sector
- Appendix 4 KILROY
- Appendix 5 STEALTH
- Appendix 6 Hex file loader
- Appendix 7 BIOS and DOS interupt functions
- Appendix 8 Suggested reading list

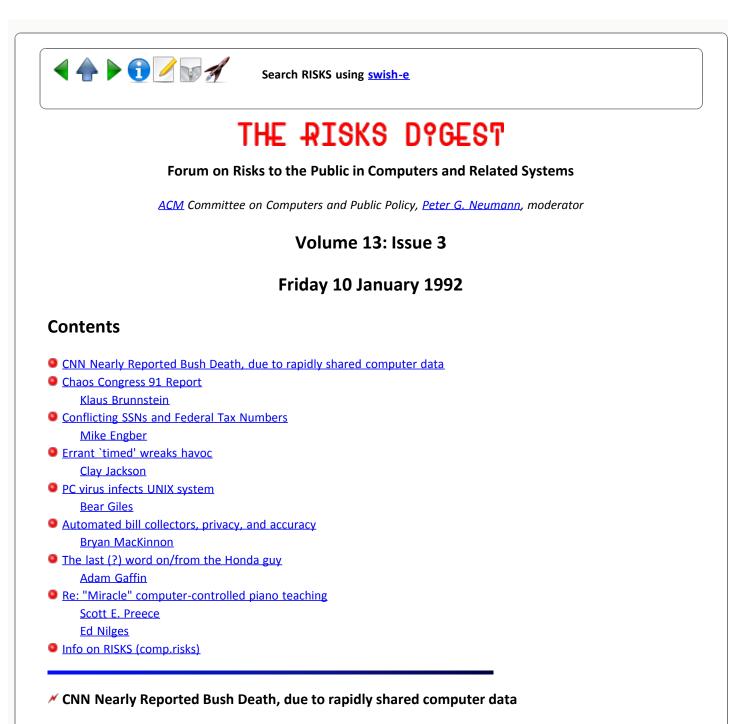
#### Kaplan's comments:

1) - "Oh,



Report problems with the web pages to the maintainer

The Risks Digest Volume 13: Issue 2



"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Jan 92 9:33:56 PST

The AP reported from Atlanta 09Jan91 that CNN Headline News came within seconds of reporting that President Bush had died at the banquet in Japan at which he had collapsed from stomach flu on 8Jan92. A caller identifying himself as Bush's doctor had telephoned CNN about three hours after Bush's collapse, and said the president was dead.

CNN and Headline News are two floors apart but use the same newsroom computer system. A staff member had typed the telephoned report into the computer. CNN executives had determined almost immediately that the report was a fake and pulled it from the computer file. But downstairs at Headline News, it had already been seen on the screen and was nearly broadcast. CNN Headline News anchorman Don Harrison started to read the report on the air at 9:45 a.m. EST during coverage of Bush's collapse, when he was alerted in midsentence by another staff member, said CNN spokesman Steve Haworth.

The alleged caller, James Edward Smith, 71, left his number with CNN and was traced to Idaho, where he was arrested and later put in a mental hospital.

[Starkly abridged by PGN]

#### Chaos Congress 91 Report

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 9 Jan 92 16:37 +0100

Report: 8th Chaos Computer Congress

On occasion of the 10th anniversary of its foundation, Chaos Computer Club (CCC) organised its 8th Congress in Hamburg (Dec.27-29, 1991). To more than 400 participants (largest participation ever, with growing number of students rather than teen-age scholars), a rich diversity of PC and network related themes was offered, with significantly less sessions than before devoted to critical themes, such as phreaking, hacking or malware construction. Changes in the European hacker scene became evident as only few people from Netherlands (see: Hacktick) and Italy had come to this former hackers' Mecca. Consequently, Congress news are only documented in German. As CCC's founding members develop in age and experience, reflection of CCC's role and growing diversity (and sometimes visible alienity between leading members) of opinions indicates that teen-age CCC may produce less spectacular events than ever before.

This year's dominating theme covered presentations of communication techniques for PCs, Ataris, Amigas and Unix, the development of a local net (mousenet.txt: 6.9 kByte) as well as description of regional (e.g. CCC's ZERBERUS; zerberus.txt: 3.9 kByte) and international networks (internet.txt: 5.4 kBytes), including a survey (netzwerk.txt: 53.9 kByte). In comparison, CCC'90 documents are more detailed on architectures while sessions and demonstrations in CCC'91 (in "Hacker Center" and other rooms) were more concerned with practical navigation in such nets.

Phreaking was covered by the Dutch group HACKTIC which updated its CCC'90 presentation of how to "minimize expenditures for telephone conversations" by using "blue" boxes (simulating specific sounds used in phone systems to transmit switching commands) and "red" boxes (using telecom-internal commands for testing purposes), and describing available software and recent events. Detailed information on phreaking methods in soecific countries and bugs in some telecom systems were discussed (phreaking.txt: 7.3 kByte). More information (in Dutch) was available, including charts of electronic circuits, in several volumes of Dutch "HACKTIC: Tidschrift voor Techno-Anarchisten" (=news for techno-anarchists).

Remark #1: recent events (e.g. "Gulf hacks") and material presen ted on Chaos Congress '91 indicate that Netherland emerges as a new European center of malicious attacks on systems and networks. Among other potentially harmful information, HACKTIC #14/15 publishes code of computer viruses (a BAT-virus which does not work properly; "world's shortest virus" of 110 bytes, a primitive non-resident virus significantly longer than the shortest resident Bulgarian virus: 94 Bytes). While many errors in the analysis show that the authors lack deeper insigth into malware technologies (which may change), their criminal energy in publishing such code evidently is related to the fact that Netherland has no adequate computer crime legislation. In contrast, the advent of German computer crime legislation (1989) may be one reason for CCC's less devotion to potentially harmful themes.

Remark #2: while few Netherland universities devote research and teaching to in/security, Delft university at least offers introductory courses into data protection (an issue of large public interest in NL) and security. Professors Herschberg and Aalders also analyse the "robustness" of networks and systems, in the sense that students may try to access connected systems if the adressed organisations agree. According to Prof. Aalders (in a recent telephone conversation), they never encourage students to attack systems but they also do not punish students who report on such attacks which they undertook on their own. (Herschberg and Alpers deliberately have no email connection.)

Different from recent years, a seminar on Computer viruses (presented by Morton Swimmer of Virus Test Center, Univ. Hamburg) as deliberately devoted to disseminate non-destructive information (avoiding any presentation of virus programming). A survey of legal aspects of inadequate software quality (including viruses and program errors) was presented by lawyer Freiherr von Gravenreuth (fehlvir.txt: 5.6 kByte).

Some public attention was drawn to the fact that the "city-call" telephone system radio-transmits information essentially as ASCII. A demonstration proved that such transmitted texts may easily be intercepted, analysed and even manipulated on a PC. CCC publicly warned that "profiles" of such texts (and those adressed) may easily be collected, and asked Telecom to inform users about this insecurity (radioarm.txt: 1.6 kByte); German Telecom did not follow this advice.

Besides discussions of emerging voice mailboxes (voicebox.txt: 2.8 kBytes), an interesting session presented a C64-based chipcard analysis systems (chipcard.txt: 3.3 kBytes). Two students have built a simple mechanism to analyse (from systematic IO analysis) the protocol of a German telephone card communicating with the public telephone box; they described, in some detail (including an elctronmicroscopic photo) the architecture and the system behaviour, including 100 bytes of communication data stored (for each call, for 80 days!) in a central German Telecom computer. Asked for legal implications of their work, they argued that they just wanted to understand this technology, and they were not aware of any legal constraint. They have not analysed possibilities to reload the telephone account (which is generally possible, due to the architecture), and they didnot analyse architectures or procedures of other chipcards (bank cards etc).

Following CCC's (10-year old charta), essential discussions were devoted to social themes. The "Feminine computer handling" workshop deliberately excluded men (about 25 women participating), to avoid last year's experience of male dominancy in related discussions (femin.txt: 4.2 kBytes). A session (mainly attended by informatics students) was devoted to "Informatics and Ethics" (ethik.txt: 3.7 kByte), introducing the international state-of-discussion, and discussing the value of professional standards in the German case.

A discussion about "techno-terrorism" became somewhat symptomatic for CCC's actual state. While external participants (von Gravenreuth, Brunnstein) were invited to this theme, CCC-internal controversies presented the panel discussion under the technical title "definition questions". While one fraction (Wernery, Wieckmann/terror.txt: 7.2 kByte) wanted to discuss possibilities, examples and dangers of techno-terrorism openly, others (CCC "ol'man" Wau Holland) wanted to generally define "terrorism" somehow academically, and some undertook to describe "government repression" as some sort of terrorism. In the controversial debate (wau\_ter.txt: 9.7 kByte), few examples of technoterrorism (WANK worm, development of virus techniques for economic competition and warfare) were given.

More texts are available on: new German games in Multi-User Domain/Cyberspace (mud.txt: 3.8 kByte), and Wernery's "Btx documentation" (btx.txt: 6.2 kByte); not all topics have been reported. All German texts are available from the author (in self-extracting file: ccc91.exe, about 90 kByte), or from CCC (e-mail: SYSOP@CHAOS-HH.ZER, fax: +49-40-4917689).

Klaus Brunnstein, University of Hamburg (Jan.8, 1991)

#### Conflicting SSNs and Federal Tax Numbers

Mike Engber <engber@aristotle.ils.nwu.edu> Fri, 10 Jan 92 14:22:17 CST

If your Social Security Number = FedTaxNumber of some business, you could be in for problems. It turns out that both SSNs and Federal Tax number are 9 digits and the government does issue Fed Tax numbers that match SSNs.

I recently tried to open an account at Savings of America, they did a credit check with ChexSystems and my SSN flagged a problem.

After 3 months, and much aggravation it turns out that some business has a Federal Tax number that is the same as my Social Security number and that business did something to get reported to ChexSystems.

I'm not sure there is anything I can do. Assuming the business really did something, the credit ding could be legit.

ChexSystems reports that the business does not have my name on it, but from the S&L's point of view it's possible I opened a business account using my SSN under the business's name name. ChexSystems won't even tell me the name of the business.

I don't really care about opening up this particular account, but I'd don't want me to come back and haunt me in the future, If anyone has any ideas, please email engber@ils.nwu.edu.

# // Errant `timed' wreaks havoc

Clay Jackson <cjackso@nv6.uswnvg.com> Fri, 10 Jan 92 13:54:36 PST

We had an interesting experience this morning with `timed' (a unix Network time daemon). A vendor brought a demonstration machine to a first-time unix user, who let the vendor install it and boot it while it was connected to our network. The machine had a `timed' set up as a master. When the vendor booted the machine, he did not set the time.

So, the first time one of our other machines on the net asked for the time, this machine responded. Soon all of our machines thought that the date was 1/1/1970. When this was first noticed, our SysAdmins found the errant machine and shut it down. Unfortunately, the story doesn't end here.

It seems that there was also a bug in our 'real' `timed' software, such that any date with more than 1 digit in the day is not handled correctly. So, the date went from 1/1/70 to 10/10/92 instantly. This caused further havoc with things like 'at' and all sorts of other unix utilities.

We're still picking up the pieces of our database (which tracks things like work orders and trouble tickets, some of which now have ages of 20+ years!).

Needless to say, we're working on a `reasonableness' check for `timed', as well as (more) controls on what gets put on our network!

Clay Jackson, US West NewVector Group Inc

### PC virus infects UNIX system

Bear Giles 271 X-6076 <bear@fsl.noaa.gov> Fri, 10 Jan 92 09:40:56 MST

We were configuring the ethernet card on our new 486 UNIX (SVR5) box when we determined that we needed to boot and run DOS to run the ethernet configuration program. (Or possibly the EISA configuration -- this happened in my office but I was not involved).

No problem: simply create a boot disk from the DOS system across the hall and reboot DOS.

Unfortunately, that system had been infected with the 'Stoned' virus. This virus overwrote the UNIX BOOT TRACK when the infected DOS was booted.

Result -- no more SVR5. We will probably have to perform a low-level format of the disk and rebuild the UNIX from original media.

Morals: 1) don't ignore DOS viruses simply because you run UNIX unless you NEVER need to use DOS. 2) Pound on DOS users to note and report strange behavior because some infections are very costly (several person-days to rebuild this system -- at least it was new and had no work-in-progress on it!)

Bear Giles bear@fsl.noaa.gov

#### Automated bill collectors, privacy, and accuracy

Bryan MacKinnon <mackinno@fndaud.fnal.gov> Fri, 10 Jan 92 09:27:43 CST

A recent incident that happend to me has called me to question the accuracy and privacy of bill collecting.

One evening, I received a phone call at home. When I answered, I was greeted by a synthetic voice stating: "Hello, I have importantant information for Jane Doe, if you are that person, please press 1 now." (I replace the real name here with Jane Doe for privacy.) I was and am not Jane Doe so I hung up. The next night, I received around the same time the same phone call - again I hang up. This went on for five days.

Sure enough, on the sixth day, my synthetic friend calls me again. Annoyed and a bit curious, I finally press 1. The voice then begins to tell me that Jane Doe, of address [not mine], had a CaT scan that has not been paid for. It gave me the date, hospital, referring doctor, and reason for the scan.

This amazed me for many reasons. I knew some very private things about a complete stranger, including a physical disorder she had (abeit minor), merely because of an incorrect telephone in a database. If the automated bill service did not have her phone number and perhaps her address correct, that could explain why she has not paid her bill.

Well, that was the last time I heard from my automated friend. I assume that the autocalling program noted that it delivered its message and it was done with its responsibility. What happened to Jane Doe, I do not know. -- Bryan.

### M The last (?) word on/from the Honda guy

Adam Gaffin <adamg@well.sf.ca.us> Fri, 10 Jan 92 08:00:00 -0800

Note comments from the man himself

Adam Gaffin, Middlesex News, Framingham, Mass. adamg@world.std.com Voice: (508) 626-3968. Fred the Middlesex News Computer: (508) 872-8461

Judge pulls the plug on Holliston man's calls, By Lisa LaBanca, Middlesex News, Framingham, Mass., 1/10/92

#### NEWS STAFF WRITER

HOLLISTON - A federal judge has hung up the Honda phone of Holliston resident Daniel Gregory. The American Honda Motor Co. has obtained a permanent

injunction in federal court that prohibits him from harassing the company.

The injunction was granted in U.S. District Court in Boston this week, according to Bob Butorac, a spokesman for the Torrance, Calif.-based carmaker. Butorac said that the Burnap Road resident signed an agreement to not telephone, send facsimile transmissions or otherwise harass the company. "It would appear that the issue is now closed," Butorac said.

Gregory, 31, made national news when American Honda decided to go to court to prevent him from calling or sending facsimile transmissions over the company's telephone lines. The company said Gregory had made more than 100 phone calls in one day last fall and transmitted multi-page letters by fax over four days. American Honda blocked off all calls to its 800 numbers from the 508 area code in order to keep Gregory from tying up the lines. ``His phone calling inconvenienced other customers who were trying to call us,'' Butorac said.

Gregory, the owner of a 1990 Honda Civic CRX, said his car did not stop properly in the rain. Gregory said yesterday {Thursday} that he would abide by the consent agreement until he disposes of the car. The agreement did not require Gregory to admit that he had harassed the company. ``In no way have I given up my quest to solve the problem,'' Gregory said. But he said the experience was useful. ``It gave me some interesting insight: I've got to be a lot more careful in not losing my cool,'' he said. ``You can compromise your opportunity to pursue a resolution if you lose your cool.''

Gregory is thinking about initiating a suit of his own: He claims that an American Honda executive contacted an area dealership and notified its management that Gregory might call them. The dealership later refused to service his car, Gregory said. ``As far as I'm concerned, he prejudiced that dealership against me.''

### Ke: "Miracle" computer-controlled piano teaching (<u>RISKS-13.02</u>)

Scott E. Preece <preece@urbana.mcd.mot.com> Fri, 10 Jan 92 09:43:54 -0600

| This is it could not recognize the slight improvisation represented by grace
| notes as an improvement over the music displayed on the screen. In my opinion,
| a good piano teacher would give Couric a higher score for the creativity
| implicit in grace notes.

That depends on whether the teacher had told her to play it as written or to perform it. Playing the instrument involves basic skills that must be mastered; performing compositions involves \*both\* those skills and aesthetic skills that have to be learned/acquired separately. It makes a lot of sense for a computer training system to grade students on their mastery of playing skills. At the present level of AI, it makes no sense at all for a computer training system to make aesthetic judgements.

Think of it as more like a typing teacher than like a music teacher.

More than this, the developers of "The Miracle" seem unaware of the fact that
Playing The Music Exactly As Written (PTMEAW) is (in a global sense) not the
usual practice. Not only is folk music almost completely improvised, Indian
classical music gains much of its richness from being IN PART improvised by

| master musicians every time it is performed.

Note the phrase "master musicians" in that last sentence. You have to earn your freedom (you're totally free to play whatever you like in your living room and grade yourself, but if you want to submit yourself for public evaluation, you'd better have the technical skills to support your improvisational insight).

Back when I lived in a city, I went to a lot of piano recitals. I would say Vladimir Horowitz made more technical mistakes than almost anyone else I heard, but was also the most riveting and persuasive of the lot. My daughter, on the other hand, though better technically and musically than most kids her age, would probably profit a lot from a mechanical grading that would not let her get away with sloppiness.

No, it won't make you a musician. That requires insight and experience. A good human teacher will help the student acquire those. But you'll never be able to express your musicianship unless you acquire the mechanical skills that something like the Miracle Keyboard \*can\* help you with.

# Ke: "Miracle" computer-controlled piano teaching (<u>RISKS-13.02</u>)

Ed Nilges <egnilges@phoenix.Princeton.EDU> Fri, 10 Jan 1992 16:45:26 GMT

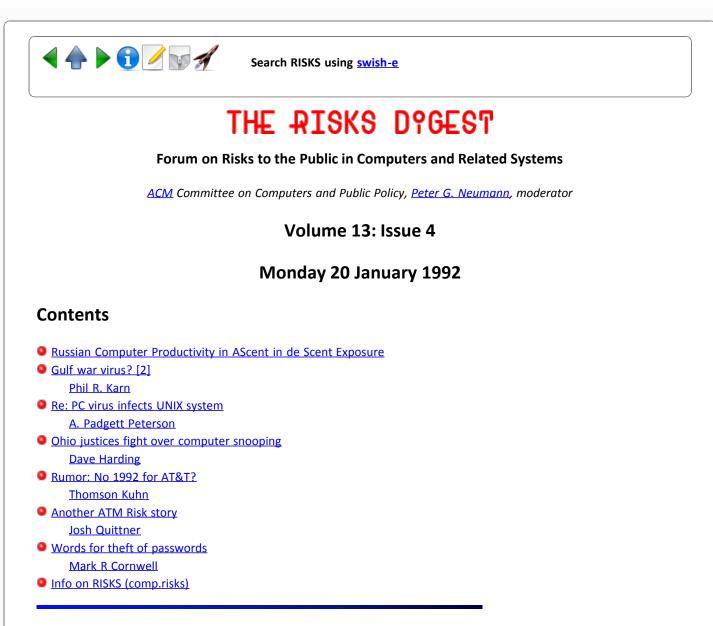
>instrumentalist in a concerto provided a "coda" in which the soloist could

Thanks to Phil Karn of the University of Chicago for correcting this post on a matter of detail. He reminded me that the improvisational section is a "cadenza" rather than a "coda", and of course a "coda" is the section in the concerto towards the end in which the soloist and the orchestra usually play "tutti." A rose by any other name and all that, and the fact remains that in a world-music sense improvisation is the norm rather than the exception (being vestigial in Western classical music through Mozart in the form of the CADENZA) but my apologies to comp.risks for this slip.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# Russian Computer Productivity in AScent in de Scent Exposure

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 20 Jan 92 14:47:38 PST

Fruit and flower smells [are] good for computer operators Moscow, 13 Jan 1992 (tass), by tass correspondent Lyubov Dunayeva

Overloads to computer operators, who have to spend hours before displays every day, can be eased if the air in the room is saturated with the smells of fruit and flowers, psychologists say. Expert experiments [!] have shown that the scent of lemon, jasmine or eucalyptus boosts productivity and alleviates drowsiness. The jasmine smell in a computer room reduces keyboard errors by almost 30 per cent, and lemon aroma by almost 50 per cent, tass was told at a surgery research center of the russian academy of sciences.

[Jasmine is clearly more saLyubrious than JazzMax. By the way, those of you who have read Nabakov's paean to programming\* language, "Ada

#### ✓ Gulf war virus?

Phil R. Karn <karn@thumper.bellcore.com> Sat, 11 Jan 92 18:34:05 EST

[The following items have stirred up considerable interest and confusion. It seems worthwhile running both the original item and its followup for those of you who missed them. PGN]

Something in this story doesn't add up. How could a "printer" infect a computer with a "virus"? [PRK]

U.S. Spies Planted Computer Virus in Iraqi Defense System

WASHINGTON (AP) \_ U.S. intelligence agents reportedly inserted a computer virus into a network of Iraqi computers tied to that country's air defense system several weeks before the start of the Persian Gulf War. The virus, U.S. News and World Report says in its issue dated next week, was designed by the supersecret National Security Agency at Fort Meade, Md., and was intended to disable a mainframe computer. Citing two unidentified senior U.S. officials, the magazine said the virus appeared to have worked, but it gave no details. It said the operation may have been irrelevant because of the allies' overwhelming air superiority.

The secret operation began when American intelligence agents identified a French-made computer printer that was to be smuggled from Amman, Jordan, to a military facility in Baghdad, the magazine said. The agents in Amman replaced a computer microchip in the printer with another microchip that contained the virus in its electronic circuits. By attacking the Iraqi computer through the printer, the virus was able to avoid detection by normal electronic security measures, the report said. ``Once the virus was in the system, the U.S. officials explained, each time an Iraqi technician opened a `window' on his computer screen to access information, the contents of the screen simply vanished,'' U.S. News reported.

The report is part of a book, based on 12 months of research by U.S. News reporters, called ``Triumph Without Victory: The Unreported History of the Persian Gulf War,'' to be published next month.

In a series of adaptations from the book, U.S. News also reported that two 5,000 pound bombs developed by the Air Force during the Gulf War, called GBU-28s, were dropped on a command bunker on the second-to-last day of the war with the explicit purpose of killing Iraqi President Saddam Hussein. The fact that the bombs were dropped Feb. 27 has been reported previously, but U.S. officials have repeatedly denied that Saddam was the intended target.

Gen. Ronald Yates, commander of Air Force Systems Command, told reporters last year that the bombs were aimed at ``senior staff'' of the Iraqi military.

U.S. News also said it had calculated, with the help of private defense analysts in Washington, that as few as 8,000 Iraqi soldiers may have been killed in the war. The U.S. government has made no official estimate of Iraqi casualties, although the Defense Intelligence Agency has said the number killed may range between 50,000 and 150,000.

I \*knew\* it sounded fishy!

Phil R. Karn <karn@thumper.bellcore.com> Mon, 13 Jan 92 15:48:46 EST

News Report of Computer Virus Attack On Iraq Is Similar To Hoax Report ROBERT BURNS, Associated Press Writer

WASHINGTON (AP) \_ A newsmagazine report that U.S. intelligence agents planted a disabling ``virus'' in an Iraqi military computer network before the Gulf War is strikingly similar to an article published last year as an April Fool's joke. The main author of the U.S. News and World Report article, Brian Duffy, said Monday, ``I have no doubt'' that U.S. intelligence agents carried out such an operation, but he said the similarities with the spoof article were ``obviously troubling.'' Duffy said the magazine was rechecking the sources who told it of the operation to determine whether details from the spoof article ``leeched into our report.'' [...]

The main elements of the U.S. News virus story are similar to an article published in the April 1, 1991, edition of InfoWorld, a computer industry publication based at San Mateo, Calif. The article was not explicitly labeled as fiction but the last paragraph made clear that it was an April Fool's joke. [...]

The U.S. News report is part of a lengthy collection of stories that it said would be published in February by Times Books-Random House as a book, titled ``Triumph Without Victory: The Unreported History of the Persian Gulf War.''

The Associated Press carried a report on the U.S. News story on Saturday, as did some other media. Questions about the story arose Monday when a number of readers called The AP to say the virus account was curiously like the InfoWorld article. That article said the virus was designed by the National Security Agency for use against Iraq's air defense control system, and that the CIA had inserted the virus into a printer being smuggled into Iraq through Jordan before the war began. ``Then the virus was on its own, and by Jan. 8, the allies had confirmation that half the displays and printers in the Iraqi air defense system were permanently out of commission,'' the InfoWorld article said.

The U.S. News report also said the virus was developed by the National Security Agency. It said that once the virus was in the Iraqi computer network, ``each time an Iraqi technician opened a `window' on his computer screen to access information, the contents of the screen simply vanished.''

The InfoWorld article also said the virus was designed to attack "window" technology in which an operator gains access to information in the computer by use of an electronic pointing device rather than typing in commands.

John Gantz, who wrote the InfoWorld article, said in a telephone interview Monday that it was fictional and that he had no knowledge of any such intelligence operation.

Duffy said he had not heard of the InfoWorld spoof. In response to an inquiry by The Associated Press, he said a U.S. News reporter in Tokyo got the ``initial tip'' on the computer virus story, which the reporter then confirmed through ``a very senior official'' in the U.S. Air Force.

Duffy said he personally confirmed the story through a senior official in the Air Force and a senior intelligence official. He said he could not reveal the three sources' names because they had spoken to U.S. News on condition of anonymity. Both the U.S. News and InfoWorld articles stressed that the reason for placing the virus in the printer was to circumvent normal anti-tampering systems in mainframe computers.

Some private computer experts said, however, that it seemed highly unlikely that a virus could be transferred to a mainframe computer from a printer.

``A printer is a receiving device. Data does not transmit from the printer to the computer," said Winn Schwartau, executive director of the International Partnership Against Computer Terrorism.

[The original report was also noted by Roland Ouellette

### Ke: PC virus infects UNIX system (Bear Giles, <u>RISKS-13.03</u>)

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com> Fri, 10 Jan 92 21:03:46 -0500

>We were configuring the ethernet card on our new 486 UNIX (SVR5) box ...

Please note that this does not mean UNIX systems are infectable by PC viruses, rather computers that use PC BIOSes can be damaged (not infected) by a certain class of PC viruses known as Master Boot Sector Infectors of which the STONED is probably the best known example.

This has been known by people who understand the architectures involved for some time. It does not mean that the STONED can infect a SPARC-station or HP/Apollo (it cannot).

What happened is that when the machine was booted with a DOS disk, the STONED being unintelligent, found the fixed disk, assumed it was another DOS disk, copied itself to absolute sector 1 and the original sector 1 to sector 7.

At this point the question becomes one of whether this actually overwrote any important data or, since the STONED changes the fixed disk access in a manner incompatible with UNIX, prevented the re-boot from acting properly (in this case all that is needed for recovery is to copy sector 7 back to sector 1. In the first case it would be necessary to rebuild sector 7 also).

For some time I have been distributing as FREEWARE two technology demonstrators: SafeMBR and NoFBoot directed at stamping out this kind of problem in the DOS world by making it impossible for MBR infectors like STONED or its clones AZUSA, MICHELANGELO, NOINT, or EMPIRE to spread. Both are tiny and only one (NoFBoot) requires any RAM (c.a. 500 bytes). They would not have prevented the damage caused to the Unix system by booting from an infected DOS disk. They would have prevented the machine "across the hall" from infecting the disk in the first place.

Padgett Peterson

ps I know they can be found on urvax.urich.edu, 141.166.1.6

# ✓ Ohio justices fight over computer snooping

Dave Harding, x2971 <HARDING@MDTF00.FNAL.GOV> Wed, 15 Jan 1992 16:03:48 -0600 (CST)

Ohio justices probed over alleged fight (Chicago Tribune, 8 November 1991)

COLUMBUS, Ohio - An investigation is under way into allegations that an Ohio Supreme Court justice angrily wrestled a fellow justice to the floor over complaints about computer file snooping, state police said Thirsday. Associate Justices Craig Wright and Andrew Douglas scuffled in front of fellow Justice Alice Robie Resnick until two of her clerks separated the pair. The witnesses said that Douglas confronted Wright over comments he reportedly had made about Douglas' secretary, Sue Pohlman. Wright said Wednesday that he and Douglas had a "little disagreement." He would not comment further Thursday. Douglas said he has been told that the State Highway Patrol is investigating.

I clipped this a while ago but didn't send it in, hoping that an Ohio correspondent would report with more details than this digested wire service bulletin offered. It is not clear who was alleged to have been doing the snooping in the others computer files. Nor is it clear whether the scuffle was over what was recorded in those alleged files or over the alleged snooping.

The question for RISKS is, as it often is, whether the incident would have happened without a computer. Would the offending notes have been made and retained? Would the other party have snooped? Would the parties gotten so excited?

### Kumor: No 1992 for AT&T?

Thomson Kuhn <70007.5444@compuserve.com> 11 Jan 92 11:11:52 EST

I have not confirmed this personally. I heard it from an AT&T VAR. He claims that no AT&T PCs can have their system dates set to 1992 via the DOS DATE command. Something about some prom code only accepting an 8 year range which ended in 1991. Further, he claims that the patch, now shipping, only provides for an additional 8 years!

Thomson Kuhn

### Another ATM Risk story, from AP

"josh quittner" <quit@newsday.com> Fri, 17 Jan 1992 12:15:30 est

NOTE: Last graf. JQ [1.800.544.5410 (2806 at tone)]

SYRACUSE, N.Y. (AP) \_ Curtis Ratliff hit the jackpot when he stuck a stolen credit card into an automatic teller machine four months ago, and it spit out \$5,600. But Ratliff's luck ran out in court Thursday when he pleaded guilty to third-degree grand larceny, the Syracuse Post-Standard reported.

In September, Ratliff stole a woman's purse from her car. The woman had left her personal identification number for the ATM in the purse along with the card. Ratliff inserted the stolen card into a grocery store ATM, which started ejecting \$20 bills, much to Ratliff's surprise. Twenty minutes later, Ratliff had stuffed \$5,600 into his pockets. ``He became blinded to the reality of what he was doing, and the money just kept coming,'' Ratliff's lawyer, James Hopkins, told the Post-Standard.

Ratliff made similar thefts at several other Price Chopper grocery store ATMs, stealing a total of \$63,900. Ratliff, 36, of Kirkville, was sentenced Thursday to five years' probation for the theft. ``I'm sorry for what I did,'' Ratliff told County Judge Patrick J. Cunningham. ``It won't happen again.''

Ratliff, who was suspended from his job as an equipment salesman after his arrest, has repaid all but \$1,800 of the money he stole, Hopkins said.

ATMs, which hold up to \$20,000, usually limit withdrawals on a single card to several hundred dollars in a 24-hour period, industry experts said. The Price Chopper machines were apparently incorrectly programmed.

#### words for theft of passwords

Mark R Cornwell -- Mind Tools Corp <cornwell@rock.concert.net> Fri, 17 Jan 92 00:19:25 -0500

This from the February 92 Atlantic Monthly column, Word Watch by Anne H. Soukhanov...

shoulder surfing -- noun, slang, the theft of computer passwords or access codes, such as long distance telephone access codes, by reading the numbers over the shoulders of authorized users: "How do outsiders discover a company's codes? by '\*shoulder surfing\*,' 'dumpster diving', and stealing calling cards" (Investor's Business Daily).

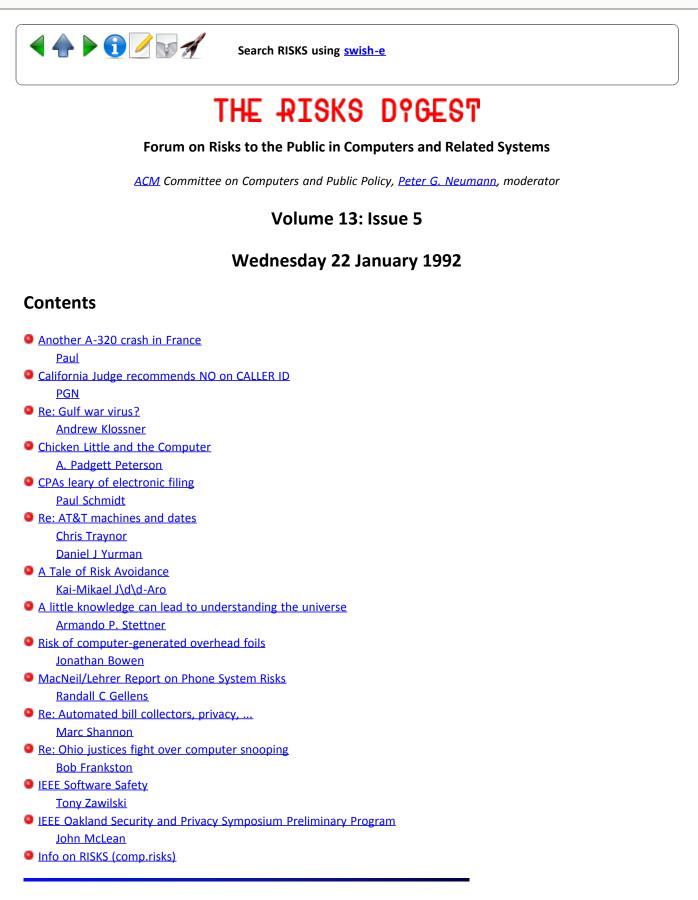
BACKGROUND: \*Shoulder surfers\* operating in the telephone marketplace are typically found in airports, train stations, and other crowded areas. In some instances they position themselves on balconies above phone booths and use binoculars to read callers' access numbers, which they later sell for \$5-\$10 each. Such fraud now costs long-distance companies some \$1.5 billion a year -- triple the damages incurred in 1985.

[Such fraud? Well, NOT JUST shoulder surfing alone... PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# Another A-320 crash in France

<"NOVA::PAUL"@yttrium.house.gov>

#### Tue, 21 Jan 1992 10:00:56 -0500 (EST)

### LATEST CRASH HEIGHTENS CONTROVERSY OVER AIRBUS A320 By Michela Wrong (REUTERS 21 Jan 1992)

PARIS, Jan 21, Reuters - The Airbus A320, a model of which crashed in France on Monday night killing 87 people, has been dogged by controversy since before its 1987 launch, with critics arguing that its computerised controls are too sophisticated. A French Air Inter A320 on a domestic flight ploughed into a mountainside in snow and fog shortly before it had been due to land at Strasbourg, giving no distress signal. Only nine of the 96 people on board survived. The narrow-bodied 150-seater became the world's fastest selling plane even before its 1987 maiden flight, notching up over 200 orders. It is central to Europe's challenge to U.S. planemakers for dominance of the world civil aviation market.

But Airbus Industrie, a consortium of French, German, British and Spanish firms, has fought to win acceptance for the advanced avionics first put to civilian use in the A320. "Each time (one crashes) the crew is blamed whereas the responsibility is really shared in the hiatus between man and machine," said Romain Kroes, secretary-general of the SPAC civil aviation pilots' union.

In a technique previously used only in combat aircraft, commands are sent electronically rather than hydraulically.

Pilots say the system restricts what they can do in a crisis by setting built-in limits on the plane's movements. They objected to a cut in the number of cabin crew on the A320 from three to two.

Airbus insists that "fly-by-wire" is safer in an emergency, allowing pilots to know how far they can push the plane without causing a disaster.

Kroes said the latest crash, which followed accidents in France and India, proved that pilots' fears were well-founded. "There are numerous faults in the way man-machine communication and the cockpit have been designed on the A320... since the Habsheim and Bangalore crashes it has been clear to us that the crews were caught out by cockpit layout," he said in a radio interview.

In June 1988, one of the first models sold to Air France crashed during a demonstration flight in eastern France. The plane cruised into a thicket of trees, killing three aboard.

A commission of inquiry accused pilot Michel Asseline of "cowboy-like behaviour" for flying too low and concluded that there was nothing wrong with the aircraft. But Asseline, who survived, insisted that the plane's equipment had failed to alert him to the loss of altitude.

A report commissioned by the victims' families found that standard procedures with flight recorders following a crash had been flouted. The main French pilots' union, SNPL, was convicted of libel for accusing the authorities of tampering with the recorders to absolve the plane and protect Airbus sales.

The controversy resurfaced in February 1990 when an Indian Airlines plane crashed at Bangalore Airport, killing 90. Indian authorities grounded all Airbuses after the Indian Commercial Pilots Association blamed a systems problem.

But a judicial inquiry concluded that the pilots were to blame for putting the engines on the wrong setting, which made the plane fly too slowly.

Airbus, which sent four experts to the scene of Monday's crash, declined to speculate on the cause, saying it would await the results of an official inquiry.

But company sources said there was no reason to think that fly-by-wire had played a role. Bad weather and the mountainous terrain were more likely factors, they said.

Created in 1970 as a European challenge to U.S. giants Boeing Co. and McDonnell Douglas Corp., Airbus has received a total of 661 orders for the A320, with 251 already delivered. The consortium of British Aerospace PLC, France's Aerospatiale, the Deutsche Airbus subsidiary of Germany's Daimler-Benz AG and Spain's CASA has 26 per cent of the world market.

The fly-by-wire technology used in the A320 is due to be adopted in a new four-engine A340 wide-body Airbus, which is being flight tested, and may also be used in a 600-seater that is in the planning stage.

[The 22 Jan 1992 San Fran Chron, p.A7, notes Agence France-Presse, citing informed sources, said that the aircraft made an abrupt 2,000-foot drop on its approach to the Strasbourg-Entzheim airport. PGN]

#### ✓ California Judge recommends NO on CALLER ID

"Peter G. Neumann" <neumann@csl.sri.com> Wed, 22 Jan 92 10:59:29 PST

California administrative law judge John Lemke has declared that Caller ID would be an unwarranted privacy invasion in an opinion that now goes to the state Public Utility Commission, which is expected to issue a final decision in the next two months. He recommended approval of other proposed services, Call Trace, Call Block, Call Return, Repeat Dialing, Priority Ringing, Select Call Forwarding, Special Call Waiting, and Special Call Acceptance, which he said could provide the benefits of Caller ID without the detriments. (Caller ID has been approved in 20 U.S. states, Washington D.C., and Canada.) [San Fran Chronicle, front page 22 Jan 1992]

### Ke: Gulf war virus?

Andrew Klossner <andrew@frip.wv.tek.com> Tue, 21 Jan 92 14:21:33 PST

"How could a "printer" infect a computer with a "virus"?"

One technically straightforward approach would be to plant the agent in a printer that will be connected directly to a network. For example, Macintosh printers are typically connected to an Appletalk network, where they enjoy full peer privileges. There is nothing to prevent such a printer from snooping around the network attempting to find and compromise other servers.

[My employer, a printer manufacturer, doesn't do this sort of thing.]

Andrew Klossner (andrew@frip.wv.tek.com, uunet!tektronix!frip.WV.TEK!andrew)

### Chicken Little and the Computer

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>

#### Tue, 21 Jan 92 10:03:40 -0500

"and so the brave little printers destroyed all of the Evil Empire's computers and they lived happily ever after." - Some of the items seen in the last year bear a remarkable resemblance to the works of Hans Christian Anderson but then it just goes to prove P. T. Barnum's axiom.

The simple fact is that the public will believe anything the public wants to believe, particularly when it deals with "magic". As a result we have printer viruses, modem viruses, CMOS viruses, and on, and on, ad nauseum. (Actually I like Aryeh Groetsky's story of a virus that infects floppy disk drives and toasters that causes both to eject their contents at lethal velocities).

This is not to say that there hasn't been a printer virus (actually a trojan - it scrambled the password in Postscript printers rendering them inaccessible), rather that information does not flow both ways (not that it can't, both zero slot LANs such as Lantastic-Z (R I'm sure) and a nifty program by Diacom (plug) that comes with a cable to connect my car's computer to a laptop and lets me find out what is going on inside utilize bidirectional communications through the parallel port) without help from a program inside the computer (I am told that Dan Jenkins, one of my favorite authors, dislikes parenthetical statements immensely).

This was the underlying problem with that Army RFP about radio transmitted viruses (understand that there were two grants made for phase one @ \$50k each): Building a virus is easy (too easy), transmitting the virus via radio is easy, the hard part is getting the other guy's computer to retrieve & execute it. Of course, if you can design the listener into the other guy's computer, you've got it made - see the French Novel "SoftWars" (not the current paperback of the same name, this one was earlier) for a description of one method. As I recall, the basis was a weather computer tied to Soviet defense systems and the program was designed so that if St. Kitts reported some impossible temperature...

Of course, the problem is that to understand what can and what cannot be done you must understand the architecture and that actually takes some research on the subject (shudder) - something abhorrent to the public and, while not unusual for a journalist, is really not what most get paid for (no-one is more ignorant than an expert speaking out of their field). Besides phone calls are more fun.

So what happens ? - a rumor starts, often innocently - like the April Fool's "InfoWorld" parody (incidentally one of the three best weekly PC magazines). However, for a parody to work it has to be just a bit off center, something obvious to experts but close enough to reality to be possible, especially when quoted out of context. In fact, as I recall, there were two similar stories at that time with the other in PC-Week).

So the rumor starts and the first thing that happens is journalists start calling up "experts" and asking "could this happen ?" with the predictable responses: "Uhhh", "If the SendMail buffer overflowed into the command queue...", "If the muffler bearings spun the transmission backwards..." and other techno-babble. Point is, it takes a lot of confidence to stand up and say "It can't happen." - besides, the journalist will then call up someone else who

will say "It could" & guess which gets printed tomorrow ?

And so the headline comes out: "Army infects Iraqi computers with virus shipped in printers from Jordan". One comment made by a neighbor (remember, my house is only a half mile from Universal Studios) during televised coverage of the Gulf War sticks in my mind: "Universal could have done it better" & the "printer virus" is a natural. - You will, Oscar, you will.

#### CPAs leary of electronic filing

Paul Schmidt <tijc02!pjs269@uunet.UU.NET> Tue, 21 Jan 92 09:28:59 EST

Several CPAs in town are not using the electronic filing offered by the I.R.S. Why? Because the I.R.S. initiates the phone call to the CPA's office to retrieve the form. This means that the I.R.S. would be accessing computers remotely. Tax preparers are worried that the I.R.S. could get more than a person's tax information by accessing all of the data on the computer.

The solution that some tax preparer's are using is to have a separate, dedicated computer for filing electronically. They put only the tax forms onto this computer. This is an easy solution since they could probably get by with just a floppy drive.

Another threat is that someone else could call the tax preparers computer and get the information.

Paul Schmidt

### Ke: AT&T machines and dates (Thomson Kuhn, <u>RISKS-13.04</u>)

<ctraynor@ATTCCS1.ATTMAIL.COM> Tue, 21 Jan 1992 11:44:36 -0500

The posting made in <u>RISKS-13.04</u> concerning AT&T machines seems to have been a little over-inflated and wrongly put by the writer. If he had indeed spoken to the VAR he would have been told that the date problem existed SOLELY on AT&T 6300 models - these were made around 83 and have 8088 CPUs. The company did not expect these machines - in their current configuration to last as long as they have (one point for us). It is a simple matter to upgrade the bios or use the date patch [Let us note that this warning is made clear to users if they ever read manuals].

I thought this list existed for the purpose of discussing risks, not for editing of the truth to make a story YOUR OWN...

Chris Traynor, AT&T Bell Labs

### Ke: AT&T machines and dates (Thomson Kuhn, <u>RISKS-13.04</u>)

Daniel J Yurman <djy@inel.gov>

#### Tue, 21 Jan 92 7:28:02 MST

In <u>RISKS-13.04</u> Thomson Kuhn notes that AT&T PCs cannot set the date to 1992. The reader may be referring to and old, and well known "feature" of the XT class AT&T 6300. This MS-DOS machine, based on the Intel 8086, had a clock chip which ran out of gas at the end of 1990. Many PC user groups have since circulated several software patches to this problem which effectively add five years to the clock chip date. These programs typically are loaded in the config.sys file and the user may merrily compute with the '6300 until the device falls apart from age.

The application to RISKS is that users, especially small businesses and home users, do not care about double declining depreciation schedules nor the technology refreshment rate of Intel-based personal computing. Once they've bought a machine this class of users has every intention of running it into the ground until it is no longer functioning, or, passing it on to their children. The manufacturer of the AT&T 6300, which as the Italian firm Oliveti, built the '6300 like a tank and mine, built in early 1986, is still surviving the assaults of four teenagers and one freelance writer. The only thing it objects to is temperatures below 65 F. Obviously, the engineers who designed the system thought any user worth his salt would give the '6300 the old heave ho within five years and so limited the clock chip accordingly.

Dan Yurman, Idaho National Engineering Lab., PO Box 1625MS 3900Idaho Falls, ID 83415Phone: (208) 526-8591Fax: (208) 526-6902

#### A Tale of Risk Avoidance

"Kai-Mikael J\d\d-Aro" <kai@nada.kth.se> Tue, 14 Jan 92 14:06:04 MET DST

[Disclaimer: I'm not trying to sell anything (in fact, none of the stuff I mention can be bought anyway), I just had a fascinating experience I'd like to share with you.]

I had been toying around with vtalk (an Ethernet-telephone for SPARC-stations from Oki Elektric Industry, Co.) and tried to add some bells and whistles to it.

Now, in the line of my studies came the exhortation "Be formal!". I have been a bit dubious of formal methods, they have seemed as a lot of sweat for obvious results. But anyway, I thought it could be nice to at least draw a little automaton so that I could have a pretty picture of all signals going back and forth between the processes of the parties.

I had Anneli Avatare, a coworker from SICS, over and we both worked for perhaps an hour drawing up an automaton on the wyteboard and trying to account for all signals. This wasn't a very large design, so after having both gone over it we were satisfied that it seemed sound.

Now Anneli suggested that we test the design in the Graphical Concurrency Workbench, GCW, on which she had worked. I had used the Concurrency Workbench before and disliked it, but the GCW was a new acquaintance. I got in to SICS the next morning, where Anneli had already drawn most of the automaton.

A little background is in order: CWB, the Concurrency Workbench is a tool developed by the Swedish Institute of Computer Science and the University of Edinburgh which allows the user to enter definitions of concurrent communicating processes and validate them, check for deadlocks, minimise the state space and so on.

As the name suggests, GCW is a graphical front-end to CWB and is implemented as an application on top of LOGGIE, a meta-tool for generating language-oriented graphical editors.

We finished up the automaton and toyed around a bit, fascinated by the (relative) ease with which we could neaten up the graph, redoing nodes and signals.

Then we got to testing the design. We created a pair of the automata and connected them to each other as the two parties.

We could then simulate the design by "sending signals" to the processes and see how little pucks moved from one state to another. To our surprise we soon managed to run the processes into a deadlock. We stared at the trace and realised we had forgotten to handle the reply signal from a sequence of hangings up and callings up. It was obvious what the fix was, and we could just add the missing vertex to the graph.

Now we tried automatic deadlock finding and watched as GCW ran through the state space moving the pucks along and found two more potential deadlock situations, both in which the fix was as trivial as in the first case.

Now, the moral of this story is perhaps not so much How Formal Methods Carried The Day And Saved My Program, but something more on the psychological side: I had been exposed to formal methods all through my professional education, but I had never realised the point of them and generally regarded them as a nuisance. Now, suddenly there was a way for me to work out the definition of a process \*interactively\*, easily amending any problems in the process, the graphic display giving me a clear picture of \*why\* my ideas were faulty, showing me \*how\* I got in the mess I was in and suggesting ways to get out of there. Perhaps the moral can be stated as: When Formal Methods Are Fun And Simplify Your Work, Then You Will Also Want To Use Them.

Kai-Mikael J{{-Aro, IPLab, NADA, KTH, S-100 44 Stockholm SWEDEN +46 8 790 91 05

### A little knowledge can lead to understanding the universe

Armando P. Stettner <aps@world.std.com> Mon, 13 Jan 92 01:03:21 -0500

While purchasing some pre-recorded cassette tapes for my mother for Christmas, the clerk placed all 15 of them down on one of those pads that have a big sign reading "Don't place credit cards or ATM cards on or near this device!"

I asked "if this thing can cause damage to the magnetic info on cards, is it safe for other things magnetically encoded to be placed on it?" After conferring with another clerk (while the tapes continued to sit on the pad), the first clerk said it is better to be safe than sorry and started to move them.

Upon hearing this short discussion, a third, more pompous clerk came over and said that these pre-recorded tapes can't be damaged by this device. She went on to say "there is this little plastic tab" on the back edge of the cassette, which, when punched out, "prevents \*any\* inadvertent erasure or recording!"

I did not know where to begin.... But clearly an example of a little knowledge can be dangerous.

aps.

### Kisk of computer-generated overhead foils

<bowen@dag.uni-sb.de> Tue, 14 Jan 92 01:01:35 +0100

A mildly amusing incident happened during the opening talk by O J Dahl today at a workshop on Software Construction here at Schloss Dagstuhl in Germany. He started his talk and a few minutes in, whilst fumbling with his foils, he suddenly realised that they had all been printed the wrong way round on the attached paper side rather than the transparency side. Always check your computer-generated slides before your talk! The replacement talk used good old hand written foils and thus avoided this (50%?!) "risk". :-)

Jonathan Bowen, Oxford University Computing Laboratory

### MacNeil/Lehrer Report on Phone System Risks

Randall C Gellens <0005000102@mcimail.com> Tue, 21 Jan 92 08:46 GMT

[Forwarded from the Telecomm Digest by <Marc\_Rotenberg@washofc.cpsr.org>] TELECOM Digest Tue, 21 Jan 92 19:31:53 CST Volume 12 : Issue 68

The MacNeil/Lehrer News Hour for Monday, January 20 contains a report (about twenty minutes or so in length) on the risks of the phone system ten years after the breakup. It includes the fire at the Chicago POP of all three carriers, the power failure in New York, the spate of software-induced outages, and lots more. Interviewed are executives from AT&T, MCI, and Sprint (the Sprint and MCI execs say how scared they were when the New York power failure hit, because if it could happen to AT&T it could happen to them), workers talking about staff cutbacks, FCC officials, Congressmen, phone users, and others. It includes footage of hearings, shots of a 4ESS, fiber trenching, and horrendous amounts of cable inside a switching center.

If you missed it live, you can order a transcript or a videotape. I forget the

address for transcripts (\$4), but the videotape number is (800ed) 328-PBS-1 (no price mentioned). (I have no connection with PBS or MacNeil/Lehrer). Randy

### Ke: Automated bill collectors, privacy, ... (MacKinnon, <u>RISKS-13.03</u>)

Marc Shannon <R602MS5U@VB.CC.CMU.EDU> Sun, 12 Jan 1992 14:05 EST

I have had a similar call to Bryan's (an automatic credit dunning system). When I received the message saying "if you are John Doe, press <1>", I pressed <1>. The system then informed me that listening to this message was an invasion of privacy and if I really wasn't John Doe, I'd be in serious trouble.

How can this be so? \*They\* called \*me\*! Don't I have the choice of what I want to do with a call that is placed to my number?

My intention in finding out that poor Mr. Doe had a credit problem was simply to find the number of the company that originated that message and inform them of the error in their database, which I did do. The woman with whom I spoke about the problem was very sympathetic to my concerns of receiving unwarranted phone calls and assured me that their database would be corrected. It must have been fixed as I have not received any more calls from them since.

The bottom line: I \*HATE\* these computer generated phone calls. If someone is calling with personal information, it had better be a person so that such errors can be detected (and apologized for) before the personal information is given out to someone it shouldn't be. At least, to the benefit of this company, they did give me a contact number. I have, in the past, received such calls telling me that I (no name given in that message) was in trouble with company X and I should send in payment immediately. They didn't leave a number to discuss it with a human.

Sigh...are we starting to rely on computers a bit much?

--Marc Shannon

# Ke: Ohio justices fight over computer snooping (Harding, <u>RISKS-13.04</u>)

<Bob\_Frankston@frankston.std.com> Tue 21 Jan 1992 16:58 -0500

Snooping is not new. What is, perhaps, new, is naivete about the accessibility of information. Back in the old days of Multics, security was viewed as a key system facility. This wasn't just because of ARPA funding, but also because the computer utility had to embody social conventions beyond those needed in a calculator. The default access to a user's information was no access. This was in keeping with the convention that one doesn't paw through another's desk. While one can argue that locking desks is not the norm, the ability to surreptitiously browse from another terminal requires something beyond simple trust.

Unfortunately, many newer systems in a misguided attempt to be friendly either ignore access control entirely or default the systems to give the world, or at least, colleagues read access.

The moderator and other readers can provide more details of the evolution of these conventions. And I'm sure newspaper staffers can tell about the entertainment of reading others' drafts.

#### IEEE Software Safety

Tony Zawilski <m16143@mwvm.mitre.org> Wednesday, 22 Jan 1992 10:44:29 EST

I am writing as Vice Chair of the IEEE P1228 Working Group on Software Safety. We have been working since October of '89 on a standard for Software Safety Plans. The SSWG has some 150 members, and we are now very close to submitting final draft to the IEEE standards hierarchy for balloting. We will be mailing out this last draft to our SSWG membership for review and comment this week. All comments would be due back at the end of February, and then the final version would be completed at our March 6 meeting. We would like to assure a broad base of comments, so if any of the readers of RISK would like to be included on the mailing list to receive this draft, please have them email their mailing address, email address, and telephone number to:

zawilski@mitre.org [ERROR FIXED in ORIGINAL MAILING] Their names will be added to the mailing list for future mailings. Thank you for your courtesy. Tony Zawilski

### ✓ Oakland Preliminary Program

John McLean <mclean@itd.nrl.navy.mil> Tue, 21 Jan 92 17:55:27 EST

1992 IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY PRELIMINARY PROGRAM

MONDAY

8:45--9:00: Welcoming Remarks: Deborah Cooper, John McLean

9:00--10:30: DISTRIBUTED SYSTEMS: John Rushby, Session Chair

- 9:00-- 9:30: On Inter-Realm Authentication in Large Distributed Systems Virgil Gligor, Shyh-Wei Luan, Joseph Pato
- 9:30--10:00: Integrating Security in a Group Oriented Distributed System Michael Reiter, Kenneth Birman, Li Gong
- 10:00--10:30: Authorization in Distributed Systems: A Formal Approach Thomas Woo, Simon Lam

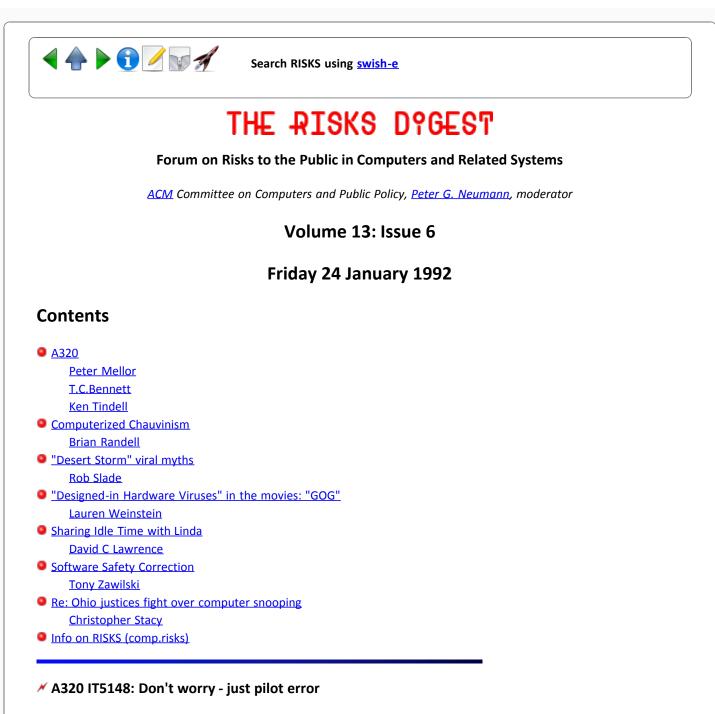
10:30---11:00: BREAK

11:00--12:00: COVERT CHANNELS: Tom Berson, Session Chair

11:00--11:30: Lattice Scheduling and Covert Channels Wei-Ming Hu 11:30--12:00: The Influence of Delay Upon an Idealized Channel's Bandwidth Ira Moskowitz, Allen Miller 12:00--2:00: LUNCH 2:00--3:00: INVITED SPEAKER: John McLean, Session Chair SPEAKER AND TITLE TO BE ANNOUNCED 3:00--3:30: BREAK 3:30--5:00: CRYPTOGRAPHIC PROTOCOLS: Dan Nessett, Session Chair 3:30--4:00: Encrypted Key Exchange: Password-Based Protocols Secure **Against Dictionary Attacks** Steven Bellovin, Michael Merritt 4:00--4:30 On Message Integrity in Cryptographic Protocols Stuart Stubblebine, Virgil Gligor 4:30--5:00: Roles in Cryptographic Protocols Einar Snekkenes 6:00: POSTER SESSIONS TUESDAY 9:00--10:30: SECURITY MODELS: George Dinolt, Session Chair 9:00-- 9:30: The Typed Access Matrix Model Ravi Sandhu 9:30--10:00: A Resource Allocation Model for Denial of Service Jonathan Millen 10:00--10:30: Non-Monotonic Transformation of Access Rights Ravi Sandhu, Gurpreet Suri 10:30--11:00: BREAK 11:00--12:00: INFORMATION FLOW: Dale Johnson, Session Chair 11:00--11:30 A Logical Approach to Multilevel Security of Probabilistic Systems James Gray, Paul Syverson 11:30--12:00 Using Traces of Procedure Calls to Reason About Composability **Catherine Meadows** 12:00--2:00: LUNCH 2:00--3:00: INTEGRITY: Richard Kemmerer, Session Chair 2:00--3:00 PANEL: Report of an Integrity Working Group Panelists: Marshall Abrams, Edward Amoroso, Leonard LaPadula, Teresa Lunt, James Williams 3:00--3:30: BREAK 3:30--5:00: CONCURRENCY CONTROL: Tom Haigh, Session Chair 3:30--4:00: A Multilevel Transaction Problem for Multilevel Secure

http://catless.ncl.ac.uk/Risks/13.05.html[2011-06-11 09:07:16]

Database Systems and Its Solution for the Replicated Architecture Oliver Costich, John McDermott 4:00--4:30: A Two Snapshot Algorithm for Concurrency Control Algorithm in Secure Multi-Level Databases Paul Ammann, Frank Jaeckle, Sushil Jajodia 4:30--5:00: Alternative Correctness Criteria for Concurrent Execution of Transactions in Multilevel Secure Database Systems Sushil Jajodia, Vijayalakshmi Atluri 5:00: TC MEETING 6:00: POSTER SESSIONS WEDNESDAY 9:00--10:30: SYSTEMS: Tanya Korelsky, Session Chair 9:00-- 9:30: Evolution of a Trusted B3 Window System Prototype Jeremy Epstein, John McHugh, Rita Pascale, Charles Martin, Douglas Rothnie, Hilarie Orman, Ann Marmor-Squires, Martha Brandstad, Bonnie Danner 9:30--10:00: A Neural Network Component For An Intrusion Detection System Herve Debar, Monique Becker, Didier Siboni 10:00--10:30: An Optimal Solution to the Secure Reader Writer Problem **Glenn Benson** 10:30--11:00: BREAK 11:00--12:00: DATABASE SECURITY: John Dobson, Session Chair 11:00--11:30: Security for Object-Oriented Database Systems Jonathan Millen, Teresa Lunt 11:30---12:00 A Natural Decomposition of Multi-level Relations Frederic Cuppens, Kioumars Yazdanian 12:00--12:15: AWARDS 12:15: SYMPOSIUM ADJOURN I 🔶 🕨 🗊 🖉 🐨 🚀 Search RISKS using swish-e Report problems with the web pages to the maintainer



p mellor <pm@cs.city.ac.uk> Wed, 22 Jan 92 16:48:30 GMT

At around 1945 local time (1845 GMT) on Monday 20th January, Air Inter flight IT5148 from Lyon to Strasbourg vanished from radar and radio contact. (In some reports the time is given as 1920 local time.) Five hours later, rescue teams arrived at the crash site on Mont Sainte-Odile (2496 feet) in the Vosges, about 30 miles south of Strasbourg. The aircraft was around 75 minutes into its flight, and about 7 minutes flying time from Strasbourg airport.

Of 90 passengers and 6 crew, 87 died, 9 survived. All of the survivors were in the rear section of the aircraft. Ten casualties were reported to have survived the impact, but frozen to death while awaiting rescue. The temperature on the ground was around -10 degrees C, there was thick fog, or cloud clinging to the mountains, and deep snow. The nearby village of Barr was used as a clearing station for the casualties.

No emergency message was received from the cockpit before impact. Survivors report that there was no prior warning, and that nothing seemed to be wrong until the impact occurred.

The emergency beacon which should have guided rescuers did not operate. According to one report, it was destroyed by the crash.

At that point on that approach to Strasbourg, the recommended height is 9000 feet, and the minimum height for a safe approach is around 4700 feet. On impact, the aircraft was below 2500 feet. Strasbourg airport is equipped with a directional beam for use by aircraft instrument landing systems (ILS). For some reason, IT5148 was not following the beam. Just before impact, the aircraft was descending at 2300 ft/min, instead of 800 ft/min (DGAC spokesman).

The flight data recorders, i.e., Cockpit Voice Recorder (CVR) and Digital Flight Data Recorder (DFDR), had been found by Tuesday night, but (according to one report) are damaged. They have been taken to Paris for examination. According to one report, they were accompanied all the way by the local examining magistrate in person.

A Commission of Enquiry has been appointed, and an interim report is expected within a month.

The pilot, Christian Hecquet, and his co-pilot had 14000 flying hours between them, but had only recently switched to the A320 from flying Caravelles. The aircraft which crashed went into service in 1988, and had a maintenance check on Monday morning.

This information has been extracted from various reports in The Guardian, The Times, The Daily Telegraph and the Daily Mail, 21st and 22nd Jan.

\*\*\*\* Above are the facts, below is the speculation. \*\*\*\*

The crash bears a certain resemblance to the previous two A320 accidents, at Mulhouse in 1988, and Bangalore in 1990. In all three accidents, the pilots seemed to think that the aircraft was higher than in fact it was.

According to the DGAC spokesman, four possible causes are being investigated:-

- "altitude computer" (FMGC? see below) failure,
- engine cut-out caused by bad weather,
- ice build-up on the wings,
- human error (in the cockpit, maintenance or ATC)

The latest crash is a serious embarrassment for Airbus Industrie, and already mutterings of "pilot error" are being heard. This is most obvious in The Times of 22nd Jan. The front page headline is:-

"Experts suspect pilot error. Crash Airbus `programmed to fly too low' "

The article (by Harvey Elliott, Air Correspondent, and our foreign staff)

#### begins:

"The pilots of an Airbus jet that crashed into a French mountain killing 87 people probably programmed the aircraft to fly too low.

As a five-man commission began its enquiry into Monday night's accident, safety experts tried to recreate on simulators the last minutes of the Air Inter flight from Lyons to Strasbourg. Their efforts suggest that the A320's "fly-by-wire" technology was not to blame."

Later in the same article:-

"Computers are capable of operating all flight controls on the Airbus, other than altitude, but David Velupillai of the manufacturer, Airbus Industrie, said: "If you program it to fly into a mountain, it will." The aircraft will prevent the pilot making a manoeuvre outside of its built-in "safety envelope", but it cannot tell the pilot that he is heading for a mountain until a few seconds before impact, when lights and buzzers alert him that he is close to the ground.

The Air Inter jet should have been at about 9,000 ft as it approached Strasbourg airport. The minimum altitude for any aircraft in that area is 4,700 ft, but the Airbus crashed into the mountainside at no more than 2,500 ft. Experts working on simulators yesterday believe that the pilot may have thought he was nearer the runway than he was, and pushed the "open descent" button that would take the aircraft to a pre-programmed altitude. Otherwise, he might have forgotten about the peaks and programmed a "normal descent" putting him on a crash course."

On page 9 of The Times, 22nd Jan., the headline reads:-

"Computer error by pilots suspected" by Harvey Elliott, Air Correspondent.

and the article goes as follows:-

"A fatal programming error by the pilots of the Airbus A320 jet which smashed into a French mountainside was emerging last night as the most likely cause of the the crash which killed all but nine of those on board.

Safety experts, anxious to discover if anything had gone horribly wrong with one of the world's most advanced passenger aircraft, took over simulators from Airbus customers around the world to try to recreate the last minutes of the flight IT5148 as it approached Strasbourg airport. Slowly, although with no real proof that their theories were right, they began to build up a picture of confusion in the cockpit.

[Stuff about minimum altitudes omitted.]

Height is the one parameter not controlled by computer in the Airbus. It is up to the pilots to tell the aircraft's five computers what height they want to fly at by dialling in a particular altitude.

The track the aircraft flies can be programmed in before take-off and the

computers then automatically follow it."

My own initial reaction to this is:-

- 1. The extension of the concept of "pilot error" to "pilot computer error" is interesting. (Not only can those dumbos not fly a 'plane, they can't even program a computer! :-)
- 2. Height is not a "parameter" which can be controlled directly, in the same way that pitch, roll, yaw and thrust are governed by the Electronic Flight Control System (EFCS) and the Full Authority Digital Engine Control (FADEC). The "five computers" referred to in the Times article above are presumably the three Spoiler and Elevator Computers (SEC) and two Elevator and Aileron Computers (ELAC) which together make up the EFCS. The pilots do not "tell" these computers anything about altitude. The Flight Management and Guidance Computer (FMGC) performs the autopilot function, and interfaces with the EFCS to cause the aircraft to follow a pre-programmed course. The FMGC \*can\* control altitude, by manipulating the EFCS. In some circumstances, the FMGC can select "open descent" mode automatically, or, on approach to an airport, the pilot can select it manually.
- 3. Unless we assume that two experienced pilots simply forgot that there are a few mountains in the way on the Strasbourg run, they would only have selected a descent mode prematurely if they did not know where they were. If they didn't, why not?
- 4. The aircraft did not "smash into a mountainside". It crashed into trees in an area where there is a fair amount of reasonably level terrain, as shown by the fact that the rear section was slowed down by the tail catching in trees. Close to impact, the altitude alarm should have started to give audible warnings at 200 ft.

Not everyone is so keen to accept the "pilot error" theory. One source was quoted as saying that, in an aircraft like the A320, pilot error lies in the "hiatus between the pilot and the computer" (lovely phrase!).

In the Times article, we read:-

"Jean-Paul Maurel, general secretary of the French pilots' union, said the aircraft had been on a normal approach path, well above the Vosges peaks when it suddenly plunged and hit the ground in less than a minute."

After 4 years in service, and 600,000 flying hours, the A320 has scored 3 major accidents and 177 lives lost. In 11 years, the Boeing 757 has flown 4 million hours with no fatalities.

As the headline to the Daily Mail feature article which quoted these statistics asks: "Is this aircraft too clever for its own good?"

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@city.ac.uk

[Also noted by Jonathan.Bowen@prg.oxford.ac.uk . ]

## Ke: Another A-320 crash in France (<u>RISKS-13.05</u>)

<T.C.Bennett@syse.salford.ac.uk> Thu,23 Jan 92 11:48:08 GMT

In <u>Risks 13.05</u> Romain Kroes, Secretary General of SPAC is quoted as saying "... it has been clear to us that the crews were caught out by cockpit layout"

Surely this statement implies that there is a problem with training rather than the software or the crew.

PGN notes an article in the San Fran Chron saying there was an abrupt drop in altitude of 2000 feet in approaching the airfield.

Since the previous two crashes of this type of aircraft seemed to be related to the altimeter it would imply that a specialised set of conditions that arises very infrequently could cause incorrect altimeter readings that indicate to the pilot that he is too high. Since both flight recorders are reported damaged we probably won't find out on this one though....

#### Thomas

Most system flaws can be attributed to unwarrantedly anthropomorphizing the user....

BITNET : ua0019%uk.ac.salford.syse@uk.ac or : ua0019%uk.ac.salford.syse%ukacrl.bitnet@cunyvm.cuny.edu

### Speculation on latest A-320 crash: why?

<ken@minster.york.ac.uk> 23 Jan 1992 15:04:47 GMT

Before we speculate over the cause of the crash we ought to bear in mind that there are vested interests in the A320. Airbus Industrie is knocking spots of Boeing and MD in sales. The US FAA can easily take the side of US manufacturers, using "software safety" as an excuse. Similarly, the French Government, which will investigate the accident, owns a share in Airbus Industrie (via Aerospatiale), and has a motive to find the accident was caused by "pilot error". There is nationalism bound up in this: Europeans are proud of the achievements of `home grown' industry, Americans are proud of their home aircraft industry. The news reports want a sensational accident to report - "Computer kills 80" instead of "Man bites Dog". Safety Critical Software researchers want to get on TV telling the world how bad computers are and "incidentally, funding of research in safety is far too low..." We should also bear in mind that the pilots' unions are concerned over the manning of modern aircraft: the 747-400 `loses' an engineer. Pilots are also concerned over the `loss of things to do'.

We should also be aware that the A320 is far from unique in having computer

control. Many many commercial aircraft have computers controlling some or all aircraft subsystems. I spent a long time a couple of years ago going through microfilm of The Times checking up on aircraft accidents. Way before the Habsheim crash I found that an DC-9 aircraft crashed from a slat/flap computer being incorrectly operated, deemed Pilot Error (August 17th 1987). The 747-400 manifested a very serious auto-throttle bug, causing loss of engine power (See RISKS 10.04).

Now, there is the very serious problem of HCl in these aircraft - the "glass cockpit" problem. The Bangalore crash (See <u>RISKS 10.48</u>) was blamed on pilot error, but it could be argued that the pilots were lulled into a false sense of security by the autopilot. It could also be argued that the training of pilots when flying in "glass cockpits" is inadequate. However, the A320 is not unique in having these problems.

Before any hysteria breaks out over computer control in aircraft (e.g. the FAA revoking the A320 license, the European aviation authorities responding by banning the 747-400, etc), we must consider what things were like before computers. In RISKS 12.72 and 13.01 the problem of the A320 Fuel Monitoring system was discussed. In olden days the re-fuelling of aircraft was a real problem. Different airports have different fuel densities, qualities, etc. Certain aircraft can only run on certain grade fuel, and whenever refuelling the technicians must know how much fuel is left and what grade it is, how the new fuel will mix with the old, and how much the new fuel will weigh (obviously, the fuel tanks have a volume capacity, whereas different density fuels will weigh different amounts) - there is an (apocryphal) story of a jet being trapped at an African airport because the fuel quality was too low. The density of fuel will change the way the aircraft is trimmed, and will change the range of the aircraft. Do RISKS readers seriously believe that ground crews with clipboards and pocket calculators made less mistakes than the A320 fuel control system?

I should point out that I am a European, and that my research (into Distributed Hard Real Time Systems) is being funded by a member of the Airbus consortium, and that my opinions are mine and no-one else's. You are free to ask whether I too have a vested interest in computer control of commercial aircraft.

Finally, I would like to quote an `expert' on aviation who in a recent TV interview said that "the common theme to all three of the A320 crashes is lack of altitude".

Ken Tindell, Computer Science Dept., York University, YO1 5DD, UK ...!mcsun!uknet!minster!ken

+44-904-433244

### Computerized Chauvinism

<Brian.Randell@newcastle.ac.uk> Tue, 21 Jan 92 18:10:47 GMT

This brief item appeared in the Jan 19 issue of The Observer, one of the "quality" national Sunday newspapers here in the UK. As a Welshman, though to my regret not Welsh-speaking, I take particular and personal exception to this

example of what I would term computerized chauvinism, though I am sure that many similar examples have been perpetrated elsewhere. Brian Randell

#### DoT HANDICAP

The Department of Transport has explained that applicants wanting driving tests in the Welsh language have been labelled 'disabled' because the computer system only has space at present under that heading. In a letter to Gwyneth County Council from its Manchester base, the Department said: 'In no way does the Department consider any person whose first language is not English as disabled.'

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

### "Desert Storm" viral myths

Rob Slade <p1@arkham.wimsey.bc.ca> Wed, 22 Jan 92 15:15:06 PST

The recent spate of reports of a virus which shut down Iraq's air defence system during "Desert Shield/Storm" seems to have started with the series "Triumph Without Victory: The Unreported History of the Persian Gulf War" by U. S. News and World Report. The articles are being rerun in many papers (as well, apparently, as CNN and ABC Nightline), and the article on the virus run in my local paper is specifically credited to USN&WR. The bare bones of the article are that a French printer was to be smuggled into Iraq through Jordan, that US agents intercepted the printer, replaced a microchip in the printer with one reprogrammed by the NSA, that a virus on the reprogrammed chip invaded the air defence network to which the printer was connected and erased information on display screens when "windows" were opened for additional information on aircraft.

The first question is: could a chip in a printer send a virus? Doesn't a printer just accept data?

Both parallel/Centronics and serial RS-232 ports are bidirectional. (Cabling is not always, and I well remember having to deal, in the early days of PCs, with serial ports which had been used as printer ports, and could not be used as modem ports because the "return" pin had been sheared off, a common practice to "fix" balky printers.) However, the "information" which comes back over the line is concerned strictly with whether or not the printer is ready to accept more data. It is never accepted as a program by the "host".

The case of "network" printers, is somewhat more complex. There are two possible cases: network printer servers and "network printers (such as the Mac Laserwriters): and they are quite distinct. The print server (on, say, DECnet) is actually a networked computer acting as a print server; accepting files from other network sources and spooling them to a printer. True, this computer/printer combo is often referred to simply as a printer, but it would not, in any case, be able to submit programs to other hosts on the net. The Mac case is substantially different, since the Mac laser printers are attached as "peers". Mac Laserwriters, at least, do have the ability to submit programs to other computers on the network, and one Mac virus uses the Laserwriter as a vector. However, it is unlikely that the Iraqi air defence system was Mac based, and few other systems see printers as peers.

Second question: if it \*was\* possible to send some kind of program from the printer to the computer system/network, was it a virus?

Given the scenario, of a new printer coming into an existing system, any damaging program would pretty much have had to have been a virus. In a situation like that, the first thing to do when the system malfunctions after a new piece of equipment has been added is to take out the new part. Unless the "chip" could send out a program which could survive, in the network or system, by itself, the removal of the printer would solve the problem.

Third question: could a virus, installed on a chip, and entered into the air defence computer system, have done what it was credited with?

Coming from the popular press, "chip" could mean pretty much anything, so my initial reaction that the program couldn't be large enough to do much damage means little. However, the programming task involved would be substantial. The program would first have to run on the printer/server/peripheral, in order to get itself transferred to the host. The article mentions that a peripheral was used in order to circumvent normal security measures, but all systems have internal security measures as well in order to prevent a printer from "bringing down" the net. The program would have to be able to run/compile or be interpreted on the host, and would thus have to know what the host was, and how it was configured. The program would then have to know exactly what the air defence software was, and how it was set up to display the information. It would also have to be sophisticated enough in avoiding detection that it could masquerade as a "bug" in the software, and persistent enough that it could avoid elimination by the reloading of software which would immediately take place in such a situation.

The Infoworld AF/91 prank article has been mentioned as the "source" for the USN&WR virus article. There was, however, another article, quite seriously presented in a French military aerospace magazine in February (which possibly prompted the Infoworld joke.) This earlier article stated that a virus had been developed which would prevent Exocet missiles, which the French had sold to Iraq, from impacting on French ships in the area. The author used a mix of technobabble and unrelated facts, somehow inferring from the downloading of weather data at the last minute before launch, the programmability of targets on certain missiles and the radio destruct sequences used in testing that such a "virus" was possible.

It has also been rumoured, and by sources who should know, that the US military has sent out an RFP on the use of computer viri as computer weapons. Although I have not seen the request, I \*do\* believe it went out, and we have confirmation in the report of a contract being awarded for further study in that area. I \*don't\* believe in the USN&WR report.

copyright Robert M. Slade, 1992 DEFMTH7.CVP 920115

PS - I have only received \*one\* report of the Mac Laserwriter virus, so don't take it as gospel. Laserwriters \*are\*, however, peers on an Appletalk net. (None of this is to be confused with the Laserwriter/Postscript password trojan/virus.)

Vancouver p1@arkham.wimsey.bc.ca | "A ship in a harbour Institute for Robert\_Slade@sfu.ca | is safe, but that is Research into CyberStore Dpac 85301030 | not what ships are User rslade@cue.bc.ca | built for." Security Canada V7K 2G6 | John Parks

### "Designed-in Hardware Viruses" in the movies: "GOG".

Lauren Weinstein <lauren@vortex.com> Wed, 22 Jan 92 13:31:39 PST

On the topic of how it would (obviously) be much easier to get your adversary's system to accept erroneous commands if you had "designed-in" such abilities, the film-conscious reader might wish to check out the science-fiction film "Gog" (1954).

In this actually above-average presentation, a top-secret U.S. space research/defense facility is plagued by a series of inexplicable "accidents". These include deaths due to runaway centrifuges, malfunctions of a giant solar mirror (ZAP!), and attacks by two utility robots ("Gog" and "Magog") which almost destroy the facility, among other major problems.

It is eventually determined that the various incidents have all been triggered by enemy forces, via a very stealthy high-altitude jet, sending signals to special receivers which were embedded within the facility's central computer by enemy agents during the computer's construction in Germany.

So keep your eyes on those printers!

--Lauren--

### Sharing Idle Time with Linda

David C Lawrence <tale@cs.rpi.edu> Thu, 23 Jan 92 09:37:15 EST

\_The\_\_New\_York\_Times\_ led its January 19, 1992, Business section with "David Gelernter's Romance with Linda", an article which discussed the massive amounts of free computing cycles available at any given moment. The thrust of the article was that these cycles could be harnessed to speed up compute intensive jobs, a general concept with which computer scientists have been working for years. Early on, however, it was alluded that sights are set on going after not only machines arranged to do the work by groups of co-operating researchers, but indeed after any machine it can access.

Several columns in it was said without even the blink of an eye:

Mr. Gelernter visualizes all these computer networks linked together --- along with all the desktop computers that are not now linked to anything. When that happens, his piece de resistance will go to work: a software program that constantly goes from computer to computer seeking out idle computer power and putting it to work.

I was a bit amazed at how directly this was offered, suggesting mostly that the only hurdles to overcome were technical ones. This even after they had already discussed the great secrecy with which some Wall Street firms are using the technology. At least several paragraphs later they got to "At Issue: Free Choice":

What is to keep Pirhana Linda or its descendants from being subverted by someone who wants to tamper with another computer or steal information? And what if an individual doesn't want to share a computer? Indeed, a generation of computer users embraced desktop technology in the 1980's precisely because they were suddenly freed from sharing a single mainframe computer with hundreds or thousands of others. [...]

Privacy experts say the issue is a broader one: being able to chose whether to participate at all.

"The critical test for any technology is whether it leaves you the ability to retreat into a private sphere," said Mark Rotenberg, Washington director for the Computer Professionals for Social Responsibility. "If you can't turn the system off, you're trapped."

Good! At least they seem to be aware of some of the risks and social obstacles they beget. But wait, there's more ...

But trends already taking hold in the computer industry are likely to SWEEP ASIDE or OVERRUN such concerns. The growth of networks is expected to continue as more and more corporate data processing executives turn to Mr. Gelernter's ideas about parallel computing.

#### [Emphasis mine.]

Now, I don't really have a problem with these executives using machines like this within their own networks, but I do have a problem with it being used more widely. I am unaware of exactly what this care-free "trends in the computer industry are", but if they do exist I hope other RISKS contributors can point them out. I had been under the impression that with the founding of organizations like the EFF and CPSR that trends within the computer society were actually better about issues like this.

Perhaps I am over-reading the scope with which "a computer program which goes from computer to computer and network to network" was offered, but even so, there seem to be many potential pitfalls which must be guarded against to prevent such a helpful migrant worker from being mutated into a rogue virus with millions of possible victims. I am quite confident that Mr. Gelernter and the others working on this project only have the best intentions in mind, but I do hope to see better how they are addressing the risks.

#### Software Safety Correction

Tony Zawilski <m16143@mwvm.mitre.org> Thursday, 23 Jan 1992 08:06:57 EST

[long message to say given email address should have been ] zawilski@mitre.ORG not .com

#### Ke: Ohio justices fight over computer snooping (Harding, <u>RISKS-13.04</u>)

Christopher Stacy <CStacy@STONY-BROOK.SCRC.Symbolics.COM> Wed, 22 Jan 1992 15:06-0500

Bob Frankston tells about the good old days of Multics, where the system defaultly enforced the convention that you don't have access to what's in your neighbor's desk.

It's worth noting that, at the same place and time, another laboratory across campus operated under a different set of social conventions.

The ITS operating system was implemented without any security. Any user could access another person's files or mailbox, or view another user's screen in real time, and in fact these practices were considered socially acceptable. In certain cases, this limited the utility of the system. For example, grading information was not usually kept on the machine. However, this open attitude and policy was generally felt to be more desirable than a secure situation, and there's no doubt that it contributed substantially to the techno-social environment there, and to the success of the laboratory.

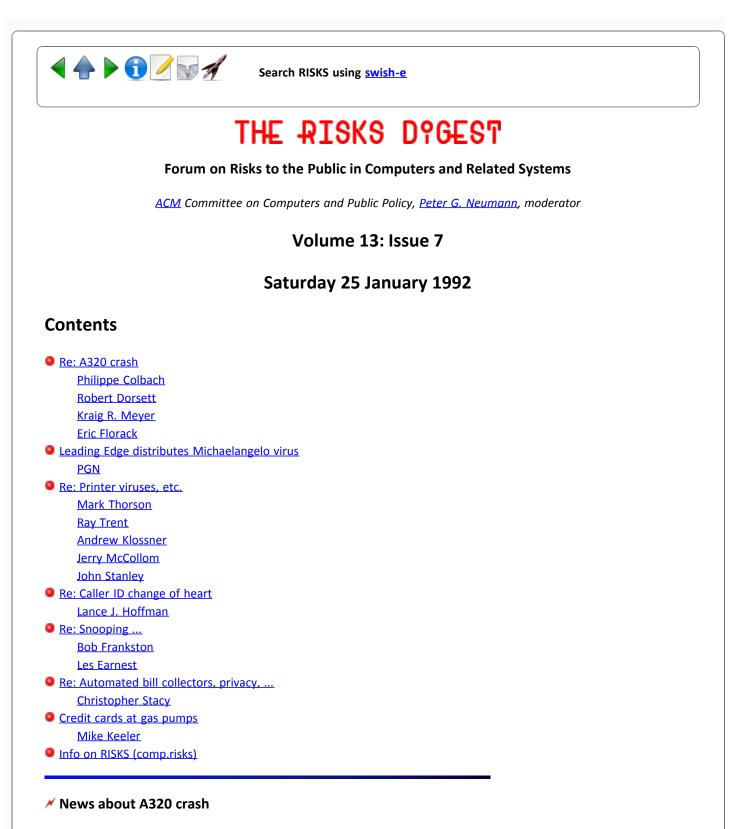
I am mentioning this here to remind us that computer environments interact with, and partially redefine, the social situations that they are intended to support. (Of course, most computer systems don't support the subtle intricacies of secrets and privacy in natural social settings. Even flexible ones like Multics are often considered by users to be too difficult to figure out how to use with the desired level of finesse.)

Computer privacy ("security") systems need to be flexible, human engineered, understood by their users, and have their policies advertised and in conformance with the social setting in which they are used. It's very easy for counter-productive security measures to infect a group's thinking - a real case of a "computer virus" infecting people! :)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Philippe Colbach <colbach@nessie.cs.id.ethz.ch> Thu, 23 Jan 1992 15:30:57 GMT

[Forwarded by John Rushby <RUSHBY@csl.sri.com>. PGN]

The German Pilot Union confirms that the European A320 does have navigation problems (abnormal behaviour of the altimeter), but ONLY during ONE of the COMMON LANDING manoeuvres, namely during the manoeuvre carried out by the

crashed A320! Lufthansa (German Airlines) admits that AIRBUS has advised all the companies using the A320 to avoid THIS landing manoeuvre, but added that there is no doubt about the security of the plane itself:

"There is no reason to withdraw the A320 from service!" the chief pilot said.

Former A320 accidents:

26.06.1988Habsheim near Mulhouse (France)Air France3 dead14.02.1990Bangalore (India)Indian Airlines90 dead

But all these accidents didn't have any impact on the success of A320! Philippe

#### Various comments on A320 posts (<u>RISKS-13.05</u>)

Robert Dorsett <rdd@cactus.org> Fri, 24 Jan 92 16:34:29 CST

T.C.Bennett@syse.salford.ac.uk wrote:

>In <u>Risks 13.05</u> Romain Kroes, Secretary General of SPAC is quoted as saying "...
>it has been clear to us that the crews were caught out by cockpit layout"

>

Surely this statement implies that there is a problem with training
 rather than the software or the crew.

No, it means there's a problem with the cockpit. There's a great tendency to fix poor interfaces by training, in the industry. The majority of a transition program, for example, is devoted to keyboarding on the flight management system, at the expense of basic skills. Indeed, there's a trend to shorten training programs, not expand them. In highly automated cockpits, there is also a well-recognized problem of the pilot being too far out of the loop; however, manufacturers do not seem inclined to change current design practices (although there are some promising refinements in the 777). This was a problem even with the "second generation" aircraft of the late 1960's; it doesn't take much imagination to see how far glass aircraft have gone. My tolerance for "fixing it through training" extends to one (1) mistake. Airliner manufacturers, however, are carrying through complete cockpit management concepts to broad families of aircraft, though, which is absurd.

ken@minster.york.ac.uk writes:

>Before we speculate over the cause of the crash we ought to bear in mind that
 >there are vested interests in the A320. Airbus Industrie is knocking spots of
 >Boeing and MD in sales. The US FAA can easily take the side of US
 >manufacturers, using "software safety" as an excuse.

But probably won't: Boeing wants to sell its 777, which is be a fly-by-wire airliner. The majority of customers will come from Europe and the Third World. The time for the FAA to take a stand was in 1987, and it didn't.

You may recall Europe dragging its heels when certifying the 747-400, in apparent retribution for the lengthy FAA special conditions for the A320 (less than a third of which dealt with the FBW control system, and even then, very superficially).

>We should also be aware that the A320 is far from unique in having computer >control. Many many commercial aircraft have computers controlling some or all >aircraft subsystems.

The 757/767/A310/A300-600 were the first generation to even step in this direction, and, as you say, all four relegated authority to \*systems\*. Safety-critical systems generally had a failsafe human interface. The airplanes all let the pilot have complete flight control.

The A320/A330/A340/777 are the first generation which genuinely filter ALL inputs through a computer. The Airbus FBW aircraft have hard limits; the 777 will have "soft" limits (which can be overridden if the pilot so desires). The latter simplifies design, and relies on pilot competence; the former assumes pilot INcompetance, and greatly increases the complexity of the code needed.

#### >The 747-400

>manifested a very serious auto-throttle bug, causing loss of engine power (See >RISKS 10.04).

To which the solution was to "click it off" and assert manual control. The autopilot, that is. It isn't clear whether one would always have the same success with the A320's full-authority digital engine control (FADEC--a central component of almost all the large fans, including the -400, but Airbus exploited the features extensively with the A320).

>security by the autopilot. It could also be argued that the training of pilots>when flying in "glass cockpits" is inadequate. However, the A320 is not unique>in having these problems.

I differ: the A320 cockpit is unique in the secure feeling it generates. I kid you not: I've been in a lot of cockpits; the A320 comes closest to being a spaceship. It has a TOTALLY insulated feel to it. Even a veteran A320-basher like myself felt decidedly cozy when I visited one a couple of years ago. The A320 pilots I know are aware of the threat, and make an attempt to fly "manual" as much as possible, with or without the airline's blessing. This concept has somewhat belatedly come to most airlines running third-generation airlines as well, which makes one wonder whether ALL the automation--which is designed to be operated from takeoff to landing, for maximum profitability--is even worth it, if nobody wants to use it beneath 18,000'.

>banning the 747-400, etc), we must consider what things were like before >computers. [...]

#### >

>Do RISKS readers seriously believe that ground crews

>with clipboards and pocket calculators made less mistakes than the A320 fuel >control system?

Yes. The issue is not reliability, it's economy.

The dispatch reliability of the A320 still lags a couple of points behind aircraft such as the 737 or 727. But it \*may\* be more profitable (the airplane is yet to deliver on a few promises). In the case of the A320 fuel control system, the issue was how best to eliminate the F/E position (at \$2 mil/year/plane in savings).

As far as the fuelling mechanism goes, the ones on the L-1011 and 747 are at least as sophisticated as the one on the A320. And, when all else fails, there're always the non-tech dripsticks, regardless of airplane. :-)

IMHO, the A320 is an aircraft with a considerable degree of notoriety (much of it exaggerated), but I think it is premature for the a320-bashers to start beating the war drums, until more information comes to light from the crash investigation. Airplanes do crash, from time to time; not every one is tied to some catastrophic flaw in design and operation.

Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd

## Software Safety (A320) and User Interface Design

## <kmeyer@aero.org> Fri, 24 Jan 92 15:07:13 PST

...Romain Kroes, Secretary General of SPAC is quoted as saying "...it has been clear to us that the crews were caught out by cockpit layout"

In <u>Risks 13.06</u>, T.C.Bennett@syse.salford.ac.uk asserts: "Surely this statement implies that there is a problem with training rather than the software or the crew."

T.C.'s statement is a popular, but inaccurate claim, among manufacturers of safety and security systems. The manufacturer will say, "It doesn't matter if that naturally lures the system administrator into leaving the system in an insecure/unsafe state--we'll put something in the manual that tells him/her NOT to do that."

An example of fatal man-machine interaction that is taught in most user interface classes is that of a plane used in WWII. In said plane, when a lever in the cockpit was up, the landing gear was down. This plane experienced a number of accidents until the manufacturer switched so that lever down=landing gear down.

There are certain things that humans naturally expect machines to do in response to certain actions, and training and manuals are not entirely successful at changing those expectations.

Kraig R. Meyer

# Re: A320 crashes: an uneducated person's thoughts; <u>RISKS DIGEST 13.06</u>

<Eric\_Florack.Wbst311@xerox.com> Fri, 24 Jan 1992 11:17:52 PST

Just some random thoughts on the subject, based on what's been posted here thus far:

<>1. The extension of the concept of "pilot error" to "pilot computer error" is interesting. (Not only can those dumbos not fly a 'plane, they can't even program a computer! :-)<<

Then how in the world did they manage to get 14,000 flight-hours between them, I wonder? It would appear that inexperience with flying in general is not a factor here.

<>3. Unless we assume that two experienced pilots simply forgot that there are a few mountains in the way on the Strasbourg run, they would only have selected a descent mode prematurely if they did not know where they were. <<

This would appear to be the best answer. Consider: If there was equipment failure either

A: the impact would have been far more sudden this this report indicates, or B: they would have radioed a mayday, since they'd have had enough time to do so.

But since, as is pointed out:

<>4. The aircraft did not "smash into a mountainside". It crashed into trees in an area where there is a fair amount of reasonably level terrain, as shown by the fact that the rear section was slowed down by the tail catching in trees.<<

it would appear that the pilots never knew that something was wrong; and all equipment appeared to be working, until it was FAR too late to do anything about it, and this is the only logical reason I've seen offered as to why they were unable to get a message off before going down.

All of this is made garbage, however, if you believe the Times article, though, where is states:"Jean-Paul Maurel, general secretary of the French pilots' union, said the

aircraft had been on a normal approach path, well above the Vosges peaks when it suddenly plunged and hit the ground in less than a minute."

This scenario would indicate some sort of major systems failure, and not the fauilt of the pilots in question. (But then, would anyone really expect a pilot's union rep to say that their members screwed up and killed X number of people in doing so?)

<>In <a href="/Risks/13.05.html">Risks 13.05</a> Romain Kroes, Secretary General of SPAC is quoted as saying "... it has been clear to us that the crews were caught out by cockpit layout"

Surely this statement implies that there is a problem with training rather than the software or the crew.<

Not being a flyer, I wouldn't know, but new equipment, particularly if there are controls in places other than where you expect them to be, or that have a different command structure to them will foul even the best of us up in a crunch. I drive a stick shift car, for example. I'm forever poking a hole in the floorboard of my wife's automatic, trying to find the clutch when I need to stop in a hurry. Some of you, I'm sure foul your typing when trying to get used to a new keyboard. Could this be a factor in this crash?

I mean, it seems established that the plane was below a safe approach level, well before the crash. Could it be, that the pilots realised this, and attempted corrective action in a hurry, and being a new system to them, fouled things up?

<>Finally, I would like to quote an `expert' on aviation who in a recent TV interview said that "the common theme to all three of the A320 crashes is lack of altitude"<<

Then, if true, could the pilot/computer interface with regards to altitude be different enough to be causing problems in panic situations?

Pure speculation, here, of course.

Final question: If the twoer was able to record that the plane was below a safe path, why was there no message radioed to the plane of the situation?

## ✓ Leading Edge distributes Michaelangelo virus

"Peter G. Neumann" <neumann@csl.sri.com> Sat, 25 Jan 92 14:14:47 PST

Between 10 and 27 December 1991, Leading Edge Products shipped up to 6000 IBM-compatible personal computer systems each of which included among the hard-disk software the Michaelangelo virus -- which wipes the hard disk on the artist's 6 March birthday, although it also has some earlier destructive effects as well. [See San Francisco Chronicle, 25 Jan 1992, p. B1]

## Another Way Printer Can Affect Host

<mmm@cup.portal.com> Sat, 25 Jan 92 11:44:40 PST

In the PC/AT environment, some adapter cards (i.e. interface circuit boards) have ROM's which contain extensions to the motherboard's own BIOS ROM for dealing with the peculiarities of accessing the interface board. These programs are executed when someone accesses the device, and could contain code which could do anything to the host system, such as writing a virus onto the hard disk. I've only seen these ROM's on graphics cards, but I think other devices perhaps including printer interfaces might have them too. Mark Thorson

#### **Ke: Printer viruses (<u>RISKS-13.06</u>)**

Ray Trent <rat@erg.sri.com> Fri, 24 Jan 92 12:12:59 -0800

It seems to me that there are many ways in which something that the media would consider a "printer" could contain a virus, or more likely a worm. The most obvious one is if the "printer" was a console printer terminal.

Some of the less obvious ones are:

The printer could simply print the wrong information. This is quite easy if you know the output is coming from some well-known program. Of course, then it wouldn't act the way it was reported to...which leads to the next possibility:

My best guess is that it's more of a meme than a virus. That is to say, an idea that you plant in the heads of your enemies that causes them to waste time checking \*everything\*, no matter how ridiculous it may be. Once you propagate the meme of a "printer virus", people without local printer technologies have to worry every time they get a printer from somewhere else, and spend time reverse engineering it (assuming that's even possible).

I often think some of the PC and Mac viruses fall into this category more than any other.

Watch what you believe, it determines who you are.

## Ke: "Desert Storm" viral myths

Andrew Klossner <andrew@frip.wv.tek.com> Fri, 24 Jan 92 12:40:45 PST

I agree that the Iraqi printer-virus story was almost certainly a hoax. But I perceive some vagueness in your explanation ...

"The print server (on, say, DECnet) is actually a networked computer acting as a print server; accepting files from other network sources and spooling them to a printer. True, this computer/printer combo is often referred to simply as a printer, but it would not, in any case, be able to submit programs to other hosts on the net."

I disagree. With a bus-style network such as Ethernet, what is to prevent a subverted print server from mimicing one of the VAX hosts? I've seen it done.

"However, it is unlikely that the Iraqi air defence system was Mac based ..." Can you substantiate this? Why is it unlikely?

"In a situation like that, the first thing to do when the system malfunctions after a new piece of equipment has been added is to take out the new part. Unless the "chip" could send out a program which could survive, in the network or system, by itself, the removal of the printer would solve the problem."

But "... a program which could survive by itself ..." is pretty much the defining characteristic of a virus: it installs itself into a new host.

"Coming from the popular press, "chip" could mean pretty much anything, so my initial reaction that the program couldn't be large enough to do much damage means little."

Indeed. In the scenario I envision, the "chip" would be a set of ROMs which fully replace the 2 megabytes of instruction storage on a PostScript printer (which is a typical size for an Adobe level 2 system such as the Laserwriter IIf.)

"However, the programming task involved would be substantial."

The NSA is capable of performing substantial programming tasks.

"The article mentions that a peripheral was used in order to circumvent normal security measures, but all systems have internal security measures as well in order to prevent a printer from "bringing down" the net."

And this security is woefully inadequate to prevent a virus that is designed with full knowledge of that security.

"The program would have to be able to run/compile or be interpreted on the host, and would thus have to know what the host was, and how it was configured."

Yes, and it seems quite reasonable that a federal spook agency would have that information.

"It would also have to be sophisticated enough in avoiding detection that it could masquerade as a "bug" in the software, and persistent enough that it could avoid elimination by the reloading of software which would immediately take place in such a situation."

But viruses do this every day!

"It has also been rumoured, and by sources who should know, that the US military has sent out an RFP on the use of computer viri as computer weapons."

The military confirmed the RFP, but pointed out that the objective of

the study was \*defense\* against such virus weapons.

-=- Andrew Klossner (uunet!tektronix!frip.WV.TEK!andrew)

## Ke: Gulf war virus? [<u>RISKS DIGEST 13.04</u>]

Jerry McCollom <jmc@cnd.hp.com> Fri, 24 Jan 92 15:17:54 MST

Fishy as the "printer virus" story is, one should note that the statment:

``A printer is a receiving device. Data does not transmit from the
 printer to the computer," said Winn Schwartau, executive director of the
 International Partnership Against Computer Terrorism.

is not necessarily true anymore. With the advent of printers that speak TCP/IP and hook directly to the network, the idea that a printer could wreak havoc on computers and networks is no longer such a far-fetched idea.

Jerry McCollom, Hewlett-Packard, Colorado Networks Division jmc@cnd.hp.com

## Ke: "Desert Storm" viral myths (Slade, <u>RISKS-13.06</u>)

John Stanley <stanley@oce.orst.edu> Fri, 24 Jan 92 14:55:00 PST

>The first question is: could a chip in a printer send a virus? Doesn't a >printer just accept data?

I read that set of articles in my copy of USN&WR, and it made me think about what a printer does and the software that drives it.

No, today's printers are vastly smarter than the dot matrix (or band printers) of yesterday. The PostScript one sitting 20 feet away is smart enough to tell the computer feeding it that it is out of paper, and not just by raising an interface signal, but by saying "out of paper". It can also tell me exactly what it didn't like about the print commands I gave it.

>However, the "information" which comes back over the
 >line is concerned strictly with whether or not the printer is ready to accept
 >more data. It is never accepted as a program by the "host".

Ah, but is that true? It was not but a short while ago that an Internet worm was released whose method of entry was to overflow the data input of a certain program, causing the extra material to be written to the stack and executed as a program. This is, I am sure, just one example of how DATA can become PROGRAM (and, as a programmer, I have had that happen too many times).

>The case of "network" printers, is somewhat more complex. ...
> ... True, this computer/printer combo is often referred to simply
>as a printer, but it would not, in any case, be able to submit programs

>to other hosts on the net.

Perhaps it could. Networked printers (the ones that hang on the Ethernet) are assigned Internet addresses just like systems are. They have access to all the information passing through the Ethernet, including passwords and login id's from remote logins.

Unless the network admin specifically excludes the printer addresses from being able to log in (if that can be done, I would have to spend some time investgating that question) there is nothing that would stop a printer from generating a login similar to one that it sees coming across the net, dumping an executable to the system, and running it.

Thinking about this, it suddenly becomes apparent the danger of terminal servers. They are capable of monitoring any login coming in through them, and the systems they talk to are unable to keep them from using it to log in 'by themselves', without also closing out the users.

>Third question: could a virus, installed on a chip, and entered into
>the air defence computer system, have done what it was credited with?

I don't recall if it was explicit or merely implied that the NSA knew what systems the Iraqi's were using. You wouldn't need to know much about the specific software, as long as you knew they were using X (a fact a smart printer could probably determine by watching the type of packets on the net) you could screw up the display.

All of this is, of course, probably highly secret and will never be known for sure. It does look like the technology is there to do something like this. Whether the NSA invested the time and effort to do it is the question.

#### Ke: Caller ID change of heart

Lance J. Hoffman <hoffman@seas.gwu.edu> Wed, 22 Jan 92 23:16:27 EST

Noting that the Kentucky Public Service Commission recently changed its mind and decided to require per-line as well as per-call blocking (Telecommunications Reports, Jan. 6), GTE said that it is now "sadly and seriously" considering withdrawing the service. Because of the uncertain status of Caller ID in several states, GTE has chosen not to file Caller ID tariffs in Arizona, Arkansas, Idaho, Iowa, Michigan, Nebraska, New York, Ohio, Oregon, Pennsylvania, South Carolina, Texas, Washington and Wisconsin.

Professor Lance J. Hoffman, Department of EECS, The George Washington University, Washington, D. C. 20052 (202) 994-4955

Ke: Ohio justices fight over computer snooping (Stacy, <u>RISKS-13.06</u>)

<Bob\_Frankston@frankston.std.com>

#### Fri 24 Jan 1992 22:37 -0500

To quote Christopher Stacy: "Computer privacy ("security") systems need to be flexible, human engineered, understood by their users, and have their policies advertised and in conformance with the social setting in which they are used. It's very easy for counter-productive security measures to infect a group's thinking - a real case of a "computer virus" infecting people! :)"

This was precisely the point of Multics access control -- developing effective security meant usable and "friendly" security. I do question whether the fishbowl atmosphere of ITS necessarily contributed to the success of the labs research. (Though there were lots of valuable ideas in (and on) ITS independent of AI and ignoring privacy issues did simplify aspects of project administration.) An organization can choose a fishbowl model and reflect it throughout the organization. To a large extent I do like the relatively open atmosphere. But we shouldn't mistake a total lack of privacy as being fundamentally virtuous.

The fishbowl approach is easy but misses the point of computer systems a part of the cultural infrastructure. I must have confidence in the privacy of email in order to use it as a fundamental means of communications and not just as a novelty. I don't discuss confidential information on my cellular phone for just that reason. The cellular phone system is a prime example of lessons not learned and a reason to periodically remind people of Camelot, oops, Multics.

The Ohio case, (given my guesses as to what happened) is another example where the fishbowl model is not appropriate.

In the PC world we have physical position as the model of privacy. This works nicely as an extension of ones desk. In order to more effectively share resources we need to have faith that the shared systems will also respect my privacy.

As an aside, I fear that misguided organizational policies may pressure people into making people contribute their machines Linda servers. After all, a CPU is a terrible thing to waste. Let's recycle them. (Luckily there are the new power management chips like the 386SL that will allow me to argue that noncomputing is nonpolluting)

Lotus Notes is a modern example of a system with a high regard for nonintrusive privacy. It achieves mixed success in regard to usability but does demonstrate how one can provide Multics-like security (and then some) in a loosely coupled PC environment. (I'll have to admit some bias here being a heavy Notes user myself).

#### Computer snooping

Les Earnest <les@sail.stanford.edu> Fri, 24 Jan 1992 23:48:51 GMT

In <u>RISKS 13.06</u>, Christopher Stacy responds to an earlier remark about

the fact that Multics normally protected files against access by others, [noting the ITS system ...].

A still different computer security scheme was in use at the Stanford A.I. Lab (SAIL) in the same period, with still different social conventions. Default file and screen protection was used and protected resources were regarded as private. However, special commands made it possible for anyone to remove any security that got in their way. Such actions "left tracks" so that questions could be asked later about why it was done. If it was done without adequate justification, social or employment sanctions were applied.

This approach probably would not work well in situations where users have little contact with each other, but in our laboratory environment it worked very well. We knew that there were enough computer security loopholes and enough smart people around who knew how to exploit them that there was no hope of strictly computer-enforced security working.

By making security-breeching software available to everyone, we levelled the playing field and diverted energies that might otherwise have been expended on creative "locksmithing" into more productive channels. The un-secure commands proved useful in a number of situations in which individuals or groups had failed to foresee the need to access certain protected files whose owners were not available.

Les Earnest, 12769 Dianne Drive, Los Altos Hills, CA 94022 415 941-3984 Internet: Les@cs.Stanford.edu UUCP: . . . decwrl!cs.Stanford.edu!Les

### Ke: Automated bill collectors, privacy, ... (Shannon, <u>RISKS-13.05</u>)

Christopher Stacy <CStacy@STONY-BROOK.SCRC.Symbolics.COM> Wed, 22 Jan 1992 14:48-0500

Marc Shannon describes a computerized telephone call from a credit agency, misdirected by a wrong phone number to him, concerning another person's account. Of course, the call violated the privacy of the intended recipient. He concludes by wondering if "we starting to rely on computers a bit much?"

Probably true in many cases, but you don't need to involve a computer for this particular problem. Although this kind of program can dehumanize the situation worse by moving you further apart, a simple answering machine will suffice. I frequently get all kinds of misdirected messages contain private information left on my answering machine; these are all different places calling different people. One popular one is for one or another doctor's office to call and leave exasperated messages telling me about how the payment for someone's particular medical service is overdue. Sometimes they bother to leave a return number. It doesn't seem to matter what the outgoing greeting on my answering machine says.

I believe that most people leaving messages simply assume that if they reach an answering machine, they have reached the correct number. Or perhaps it has little to do with technological risks, and is instead really a social issue. For example, maybe these kinds of incidents can be attributed to people just

not caring about the quality of their work, rather than to technological naivete. Perhaps these problems contribute to each other.

One risk that we run in RISKS, is attempting to analyze broad social issues with our pronounced technocratic tendencies.

## Credit cards at gas pumps

<mike@bitbkt.alisa.com> Fri, 24 Jan 92 15:54:59 PST

A gas station near my house recently added credit card readers to their gas pumps so one no longer has to go inside to pay.

At first I thought it was convenient. It even gave me a little receipt. How special.

I went home and thought I'd calculate my gas mileage. I whipped out the receipt and noticed that it was for \$2.00 less that what I had put in. Hmmm, that's strange. Then I noticed that it was somebody elses card number and name on the slip. I had watched the receipt print, so I know it wasn't the case of someone not taking it after the sale.

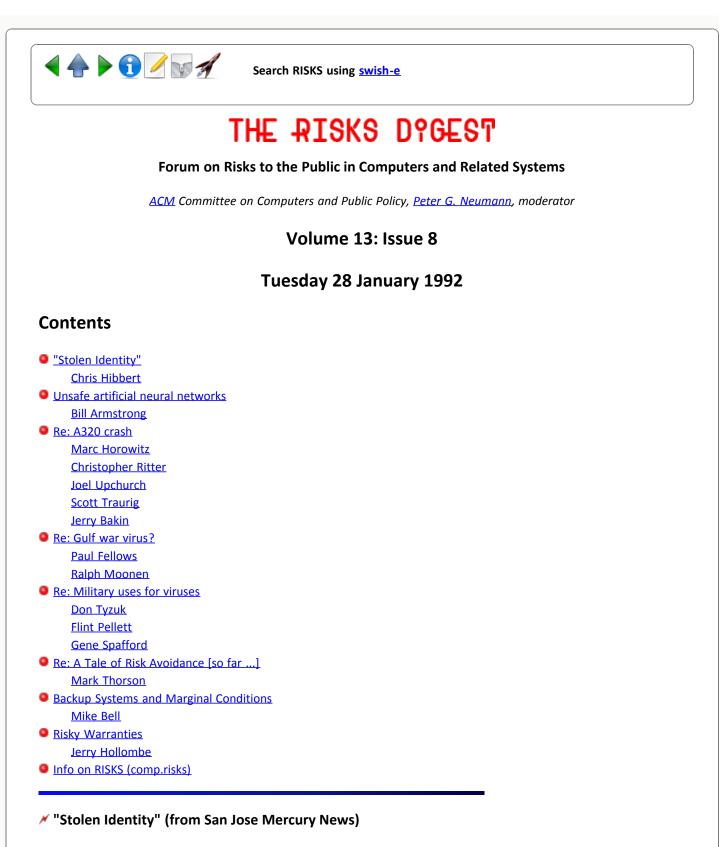
If I got someone elses receipt, maybe that person got mine. Somehow, I don't get a warm fuzzy feeling from that. Sounds like a risk to me...

Mike Keeler, Alisa Systems, Inc., mike@alisa.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<hibbert@xanadu.com> Mon, 27 Jan 92 17:46:14 PST

There was an article in the San Jose Mercury News, 12 January 1992, titled "Stolen Identity", that should be of interest to RISKS readers. It concerned a woman who had numerous driving infractions charged to her because an unscrupulous aquaintance was able to get away with supplying the woman's

driver's license instead of her own. Here's a summary:

One woman (Donna) lets another, down on her luck, (Billy) live in her apartment for a few months till she gets back on her feet. Billy finds out Donna's Drivers License number, and proceeds to give it any time she is stopped by the police, which happens quite a lot. The police take Billy's word for her name, and Donna is unwittingly saddled with tickets from Police Departments in Oakland, San Mateo, Santa Clara, and San Jose as well as the CHP. Early in the game, an officer may have allowed her to see the results of looking up the license number in the databases accessible from the squad car. Donna has tickets for speeding, expired registration, open containers of alcohol, going through stoplights, failure to wear a seatbelt, and of course driving without a license.

Donna has given up on fixing the problem, and has cancelled her license. Her last hope is that some cop will arrest Billy for the more serious charge of driving with a suspended license.

Chris

### ✓ Unsafe artificial neural networks

Bill Armstrong <arms@cs.ualberta.ca> Mon, 27 Jan 1992 18:43:45 -0700

Here is an example of a backpropagation neural network that has very wild behavior at some points not in the training or test sets. It has just one input unit ( for variable x), two hidden units with a sigmoidal squashing function, and one output unit.

This kind of subnetwork, a "neural net virus" if you like, may exist in many of the networks that have been trained to date. It could be built into any large BP network, and might hardly change the latter's output behavior at all -- except in one small region of the input space, where a totally unexpected output could occur that might lead to disaster.

I hope this note will be taken as a warning by all persons whose ANS are used in safety critical applications in medicine, engineering, the military etc. It is also an encouragement to design safety into their neural networks.

In order to avoid details of the backpropagation algorithm, we shall just use the property that once a BP net has reached an absolute minimum of error on the training and test sets, its parameters are not changed. So our net will have zero error by design and the BP algorithm, applied with infinite precision arithmetic, would not change its weights. The issue of getting stuck at a local minimum of error does not apply in this case, since it is an absolute minimum.

All the weights in the system remain bounded, and in this case, the bound on their absolute values is 40. The output unit's function is 40 \* H1 + 40 \* H2 - 40, where Hi is the output of the i-th hidden unit (i = 1, 2). The output unit has no sigmoid, though one could be inserted with no loss of generality. The two hidden units have

outputs of the form  $1/(1 + e^{(w0 + w1^*x)})$  with w0 = -10 and w0 = 30, while w1 = +40 and -40, respectively.

We assume the net has been trained on a subset of integers and also tested on a subset of integers. This could be replaced by a finer grid, and safety assured (for bounded weights). However, in a d-dimensional input space with a quantization to L levels of each variable, one would need L ^ d training and test points, which can easily be an astronomically large number (e.g. 1000^10). Hence it is not generally feasible to assure safety by testing.

Below is the overall function f(x) produced by the net, which is also the specification of what it is \*supposed\* to do outside the interval (0,1). In (0,1) the specification is to be less than 0.002 in absolute value.

 $f(x) = 40 [ 1/( 1 + e^{40*(x - 1/4)}) + 1/( 1 + e^{-40*(x - 3/4)}) - 1 ]$ 

The largest deviation of our trained network f(x) from 0 on all integers is

f(0) = f(1) = 0.0018...

So f is within 2/1000 of being 0 everywhere on our training and test sets. Can we be satisfied with it? No! If we happen to give an input of x = 1/2, we get

f(1/2) = - 39.99...

The magnitude of this is over 22000 times larger than anything appearing during training and testing, and is way out of spec.

Such unexpected values are likely to be very rare if a lot of testing has been done on a trained net, but even then, the potential for disaster can still be lurking in the system. Unless neural nets are \*designed\* to be safe, there may be a serious risk involved in using them.

The objective of this note is \*not\* to say "neural nets are bad for safety critical applications". On the contrary, I personally believe they can be made as safe as any digital circuit, and a lot safer than programs. This might make ANS the method of choice for safety-critical electronic applications, for example in aircraft control systems.

But to achieve that goal, a design methodology must be used which is \*guaranteed\* to lead to a safe network. Such a methodology can be based on decomposition of the input space into parts where the function synthesized is forced to be monotonic in each variable. For adaptive logic networks, this is easy to achieve. The random walk technique for encoding real values used in the atree release 2.0 software available by ftp is not appropriate for enforcing monotonicity. Instead, thresholds should be used, which are monotonic functions R -> {0,1}. By forcing monotonicity, one can assure that no wild values can occur, since all values will be bounded by the values at points examined during testing.

For BP networks, I am not sure a safe design methodology can be developed. This is not because of the BP algorithm, per se, but rather because of the architecture of multilayer networks with sigmoids: \*all\* weights are used in computing \*every\* output (the effect of zero weights having been eliminated). Every output is calculated using some negative and some positive weights, giving very little hope of control over the values beyond the set of points tested.

Prof. William W. Armstrong, Computing Science Dept., University of Alberta; Edmonton, Alberta, Canada T6G 2H1 Tel(403)492 2374 FAX 492 1071

#### Ke: News about A320 crash (Colbach, <u>RISKS-13.07</u>)

Marc Horowitz <marc@Athena.MIT.EDU> Sun, 26 Jan 92 23:00:17 EST

<> Lufthansa (German Airlines) admits that AIRBUS has advised all the <> companies using the A320 to avoid THIS landing manoeuvre...

Given the description of the local geography, it sounds like this either means you use this landing maneuver (guess which side of the pond I'm from :-), or you don't land A320's at Strasbourg. Is this a RISK of bugs in flight software affecting seemingly unrelated things, such as airline equipment schedules?

Marc

#### 🗡 Re: A320 crash

Christopher Ritter <critter@garnet.berkeley.edu> Sun, 26 Jan 92 23:33:58 -0800

The localization of "pilot error" in "the hiatus between the pilot and the computer" is a more solidly persuasive notion than the slick equivocation of the phrase might suggest.

As I understand it, control of the A320 is mediated by flight control computers differently in one dimension (the vertical) than in the other two. Why is this the case? Is particularly different status given to altitude, in terms of attentional demands on pilots, compared to the aircraft's motion in the other two dimensions? Or, must A320 pilots attend to and control altitude in a manner different from what is for them either customary or sensible?

Re the overall FBW design, if pilots circumvent, push the limits of, tweak or otherwise attempt to assert as much direct control over the aircraft as possible, working against the "hard," "soft" or whatever degree of automated mediation imposed by the computers, the problem is one caused not by pilot or aircraft as such, but by the designers.

Germane to this, in cognitive psychologist Don Norman's (1988) The Design of Everyday Things (aka The Psychology of Everyday Things), he writes:

Aircraft designers started using meters that looked like clockfaces to represent altitude. As airplanes were able to fly higher and higher, the meters needed more hands. Guess what? Pilots made errors- serious errors. Multihanded analog altimeters have been largely abandoned in favor of digital ones because of the prevalence of reading errors. Even so, many contemporary altimeters maintain a mixed mode; information about rate and direction of altitude change is determined from a single analog hand, while precise judgments of height come from the digital display.

Some relevant questions about the A320 flight deck should be obvious. Norman continues:

Automation has its virtues, but automation is dangerous when it takes too much control from the user. "Overautomation"- too great a degree of automation- has become a technical term in the study of automated aircraft and factories. One problem is that overreliance on automated equipment can eliminate a person's ability to function without it, a prescription for disaster if, for example, one of the highly automated mechanisms of an aircraft suddenly fails. A second problem is that a system may not always do things exactly the way we would like, but we are forced to accept what happens because it is too difficult (or impossible) to change the operation. A third problem is that the person becomes a servant of the system, no longer able to control or influence what is happening....

All systems have several layers of control.... Sometimes we really want to maintain control at a lower level... At other times we want to concentrate on higher level things....

So the question is, what is the level of control that is appropriately accorded aircraft pilots, based upon how humans think, on how pilots actually behave?

Relevant references from Norman's biliography list might also be:

Hurst, R. & Hurst, L.R. (Eds.) (1982). Pilot Error: The human factors. London: Granada.

Weiner, E.L. (1980). Mid-air collisions: The accidents, the systems and the realpolitik. Human Factors, 22, 521 - 533. Reprinted in Hurst & Hurst.

- Weiner, E.L. (1986) Fallible humans and vulnerable systems: Lessons learned from aviation. (To be published in Informations Systems: Failure analysis. Proceedings of a NATO Advanced Research Workshop on Failure Analysis of Information Systems.)
- Weiner, E.L., & Curry, R.E. (1980). Flight-deck automation: Promises and problems. Ergonomics, 23, 995 1011. Reprinted in Hurst & Hurst.

Christopher Ritter, Education in Math, Science and Technology Program School of Education, University of California at Berkeley, Berkeley, CA 94530

### ✓ Speculation on latest A-320 crash: why?

## Joel Upchurch <joel@peora.sdc.ccur.com> Mon, 27 Jan 1992 07:56:05 GMT

I have a much simpler theory for why the A-320 has had so many crashes so far. My experience is that the fewer number of events that have to occur to cause a particular error the more likely that error is to occur. It seems to me that if the pilot makes an error that isn't immediately fatal, then most of the time the co-pilot is going to catch the mistake before it is fatal. Let us say that the co-pilot catches 90% of the pilot's mistakes. So one time out of ten the co-pilot misses the pilot's mistake and the plane crashs. Let us assume that in a plane with a three man crew that the flight engineer also will catch the pilot's mistake 90% percent of the time. It seems to me that the chance that both of them would miss the error would only be 1%, that is the rest of the flight crew would catch the pilot's error 99 times out of 100. Now I know this is a gross oversimplification and the actual ratios are wrong, but qualitatively the idea feels right. There is just one less pair of eyes and ears in the cockpit to notice that something is wrong.

One thing that might support this is to study the relative accident rates of large airlines that would generally have three crew members, commuter airlines that would probably have two and air taxis and general aviation, that would probably only have one pilot. The difference might not entirely be due to the difference in the experience of the pilots. It might be informative to compare the A-320 accident rates to other planes that have a two man crew, rather than comparing it to planes of similar size that use a three man crew.

Also has anyone ever broken aircraft accident rates down to the rate per landing and takeoff? It seems to me that might be more informative than aircraft-hours or aircraft-miles.

Joel Upchurch/Upchurch Computer Consulting/718 Galsworthy/Orlando, FL 32809 joel@peora.ccur.com {uiucuxc,hoptoad,petsd,ucf-cs}!peora!joel (407) 859-0982

### Situational Awareness and the A320 (Dorsett, <u>RISKS-13.07</u>)

Scott Traurig <traurig@ncavax.decnet.lockheed.com> Mon, 27 Jan 92 08:42:21 EST

I am a great admirer of the A320, and, while I am not a pilot, I enjoy a similar level of automation when navigating the 35' sailboat I race on every summer. The equipment I use works extremely well, but if you punch in the wrong numbers it will take you to the wrong place just as fast as it would to the correct one. Although double and triple checking your work and monitoring the progress of your vessel should always be done, the technology for "getting you there" has greatly outstripped the technology for "telling you where you are, and where you are going", i.e., situational awareness.

Although you can easily read latitude, longitude, altitude and airspeed from your instruments, the method for relating this to possible hazards to navigation is still primarily a manual one. Now that pilots are becoming "system managers", they need to have the tools to monitor the system as a whole, not just the hydraulic and mechanical subsystems. Simple ways to improve upon this might include a vertical profile display on one of the cockpit CRTs that plots both the programmed flight path of the aircraft and the altitude of the ground from zero to five minutes into the future, and a moving map display that also shows the predicted flight path. I know that on the boat I race on I would dearly love to have the Trimble moving map display that does this, it would significantly reduce my workload.

Scott (traurig@ncavax.decnet.lockheed.com)

#### Re: the Airbus crash

Jerry Bakin <JERRY@INNOSOFT.COM> Sun, 26 Jan 1992 21:09 PST

Regarding the Airbus crash. It has been noted that altitude is the one parameter the pilots cannot program in.

Altitude maybe the most important parameter. Perhaps it is better that the pilot-programmers program in altitude and let the computer derive the rest of the information. The question may be which piece of data is crucial to the problem and which is an artifact of antique technologies and obsolete methods.

If I were specifying a fly-by-computer system, I would certainly require a database of all relevant altitudes (elevation at 100 foot intervals, airports, minimum operating altitudes, etc).

Certainly with today's INS and GPS Systems, there is no more reason for a computer controlled plane to fly into the ground then for a cruise missile to overfly its target. Say how much software does the Airbus and the Exocet share?

Jerry Bakin. Jerry@Innosoft.COM

#### M DNA Dogtags - followup

David States <states@artemis.nlm.nih.gov> Fri, 24 Jan 92 03:26:11 GMT

Some followup on the earlier posting I made regarding the U.S. Army's proposal to use "DNA dog tags" to build a database of soldiers genotype's as a universal identification resource.

The New York Times (Jan. 12, pp. 15 "Genetic Records to Be Kept on Members of Military") reports that the Army will go forward with the idea incorporating a number of protections for the genetic privacy of soldiers. First, they will only collect DNA samples (blood spots), but they will not genotype them unless there is an actual need. Second, these samples will be destroyed when the individual leaves the military. Finally, and perhaps most importantly, these samples will be treated as "medical specimen with confidentiality and respect," so they would not be available for testing for other purposes unless subpoenaed by court order.

The net effect of these protections is about as much as could be hoped for. The military will be able to use a valuable new technology in identifying the remains of soldiers, and they will be able to do this without creating a massive electronic database of genotype data.

Meanwhile, the British journal Nature reports an anecdote which illustrates some of the pitfalls and prejudices of dealing with genetic data, "Challenge to British forensic database" Nature, vol. 355, p.191. Since you can't change your genes, the data in a genotype database will never go out of date, right? Well it appears that is what the Metropolitan Police believed. Scotland Yard has been building a database of genotypes from all the DNA samples they have analyzed in the course of various criminal investigations. The problem is that when a man cleared of all charges on the basis of a DNA analysis asked to have his profile removed from the database, they found it necessary to "call in a computer specialist." It seems that in designing the database, no one had considered the possibility that you might want to delete an entry.

David States, National Library of Medicine

#### Ke: Gulf war virus? (<u>RISKS-13.05</u>)

Paul Fellows <paulf@mcanix.inmos.co.uk> Mon, 27 Jan 92 16:27:26 GMT

If the printer was a SCSI Printer, it could do the following :-

1) Change from Target mode to Initiator mode.

Most SCSI controllers support both initiator and target modes.

2) Interrogate each device on the bus to find the boot disk.

It may choose not to select ID 7 as this is probably the host ID.

3) Write the virus directly to the boot disk (or indeed any other disk).

Some SCSI devices can even have their firmware downloaded across the SCSI Bus. A rogue program could download a virus that infects the disk as described above. Therefore the O/S ought to prevent direct low level access by user software to any SCSI device!

The company I work for does not make printers.

Paul Fellows, Inmos Limited, 1000 Aztec West, Almondsbury, Bristol, BS12 4SQ, UK. uunet!inmos.com!paulf EMail(UK) ukc!inmos!paulf

## Enough of printers... (<u>RISKS 13.0[67]</u>)

<rmoonen@hvlpa.att.com>

Mon, 27 Jan 92 08:40 MET

So, could we please stop the discussion right here? I mean, we got two sides:

"Well, assuming 1,2,3 and 4 it might very well be possible for a printer to spread a virus throuh a network"

"Nah, never. Printers are used to print stuff. The programs in printers would never be able to do such a thing"

Regardless of who is right, maybe the discussion should focus on a way to make sure that 1 2 3 and 4 do not occur anytime. To me it seems very unlikely that such a thing occured in the Gulf war. But maybe, just maybe, someone got the idea, and has just now finished his first compile.....

So the real RISKS in my opinion is not "has it happened" but "what will be the consequences when it does happen".

I'm already giving my printer strange looks every time my job doesn't come out as I want it to be :-)

--Ralph Moonen, rmoonen@hvlpa.att.com

### Military uses for viruses

Don Tyzuk <841613t@aucs.acadiau.ca> Sun, 26 Jan 1992 12:44:25 GMT

About the military uses for viruses:

To ensure defeat of the enemy, a military commander will use every weapon at his disposal, to exploit all weaknesses. The computer systems that are necessary to operate an air defence network are obviously a weak link.

If the lives of Allied aircrew can be saved by a computer virus, then that option would appear very attractive to the Commander in Chief.

Anyone reading this can believe that maximum effort was made to to exploit all weaknesses.

Donald Tyzuk, P.O. Box 1406,Wolfville, Nova Scotia, CANADA BOP 1X0+1 902 542 7215

### Ke: "Desert Storm" viral myths

Flint Pellett <flint@gistdev.gist.com> 27 Jan 92 22:18:54 GMT

If the NSA got ahold of a piece of hardware that was going to be used in an Iraqi computer network that was supposedly secure, I would expect that there are lots of things they could do with it that would be far more helpful to us or damaging to them than messing around with a virus, and a lot easier to do besides. For example, a printer connected to a network could be set up to broadcast everything coming across the network in some fashion, or for that matter it might glean info merely by broadcasting any talking it picked up near the printer.

Flint Pellett, Global Information Systems Technology, Inc., 100 Trade Centre Drive, Suite 301, Champaign, IL 61820 (217) 352-1165 uunet!gistdev!flint

#### 🗡 Re: Viruses & printers

Gene Spafford <spaf@cs.purdue.edu> 28 Jan 92 18:10:37 GMT

Well, as so many other people are indulging in speculation, I might as well join in. :-)

First, we should consider some things about the likely target of such an attack, if it happened. First, it is unlikely that the system involved was a general-purpose system with programs out on disk that could be run, one at a time. It is also doubtful there was any such thing as a peer printer on a network link.

Why do I say that? Because the alleged system was for air defense. This means it was a system with a strong real-time component. In general, systems such as this are built on older, more stable hardware and involve an embedded system -- not a disk full of utility programs like your favorite Unix or VMS time-share environment.

The idea of a virus in such a system is ludicrous. Viruses don't work in embedded systems. That, coupled with the general press's inability to tell a virus from a spreadsheet, leads me to believe it certainly wasn't a virus, if it was anything.

However, if we care to speculate a bit further, consider the possibility of a small Trojan horse being built into the air defense software by the original contractor. Now imagine that a printer is brought in to the system that has a small radio receiver involved, so that when a certain coded signal is received, the printer uses a timing channel to signal the trojan in the printer driver that it is time to disrupt operations. This is particularly easy in an embedded, real-time system. Suddenly add a 5-second delay loop, for instance.

This is certainly within the realm of possibility. Furthermore, it would be harder to detect under test (timing channels are notoriously difficult to find, but are well-suited for certain real-time systems) without actual source code, and it would not have the same hit-or-miss qualities of a virus. (Even source code might not help, if we keep Thompson's little cc/login escapade in mind.)

April Fool's joke or not, don't believe the press when they say "virus" -- but don't automatically believe they don't have a story underneath the mistakes, either!

Gene Spafford, NSF/Purdue/U of Florida Software Engineering Research Center,

Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-1398

## Ke: A Tale of Risk Avoidance [so far ...]

<mmm@cup.portal.com> Fri, 24 Jan 92 00:38:30 PST

"Kai-Mikael J\d\d-Aro" <kai@nada.kth.se> says in <u>RISKS DIGEST 13.05</u>:

> Perhaps the moral can be stated as: When Formal Methods Are Fun And Simplify> Your Work, Then You Will Also Want To Use Them.

This might not be an unmitigated success, from the RISKS point-of-view. For example, when the transition occurred from assembly language to compiled languages, people found they could solve their old problems more easily. They could say a + b = c without even knowing the address of a, b, and c.

The problem is that compiler technology (known in the old days as "automatic programming") gave the individual programmer more reach. It allowed him to attack problems beyond his mental grasp in the pre-compiler era.

Tools will always be pushed to their limit, because the limit is actually in the programmer and it is the fundamental nature of programmers -- like athletes -- to go as far as they are capable, and try to go a bit farther. The tool simply provides an amplification, like giving a pole-vaulter a longer pole. The RISK is that the new tool allows the programmer to do more damage than before.

Will Kai-Mikael J\d\d-Aro find himself next year creating state diagrams with the complexity of a street map of Stockholm with 100 pucks circulating around it? This might open a whole new range of computer applications (like, say, an automatic vehicle control system for the streets of Stockholm), but there is no particular reason to believe these systems will be more reliable than the smaller systems built before the tool was developed. The RISK is that these larger and more complex applications will cause more damage when they fail.

Mark Thorson (mmm@cup.portal.com)

## Mackup Systems and Marginal Conditions

Mike Bell <mb@sparrms.ists.ca> Thu, 23 Jan 92 09:34:51 EST

A snowstorm here in Toronto last week caused a "brownout" that revealed an interesting failing in our emergency lighting system.

The emergency lighting is supplied by boxes containing batteries with a pair of spotlights mounted on top. These are plugged into sockets around the building. The idea is that if the mains supply fails, the lights will turn on.

When the mains supply voltage dropped, most of the fluorescent lighting failed.

However, the drop was insufficient to trigger the emergency lighting, which remained (mostly) off. Fortunately the units could be unplugged to trigger the lighting.

Also of note was a PC, which failed to detect the power problems and continued operation when the rest of the computers shut down. I'm not sure if this was an advantage (doesn't lose your work in the event of a brownout) or a disadvantage (doesn't react to power problems which may damage the computer).

#### Kisky Warranties

The Polymath <hollombe@soldev.tti.com> Fri, 24 Jan 92 14:47:38 PST

Here's a risk from the software industry that seems to have bled into other areas with the help of no less than our own Federal Government.

We've all heard, joked and complained about -- and suffered with -- software warranties that do far more to protect the vendor than the buyer. Loosely, they can be summed up as saying 'We warranty that there are recoverable bits on this disk. Beyond that, you're on your own.'

I recently made some substantial (~\$1300) purchases of a couple of non-computer products. Imagine my feelings at finding the following familiar seeming words on the backs of the associated user's manuals (manufacturers and products have been concealed to protect the guilty):

WHY NO WARRANTY CARD HAS BEEN PACKED WITH THIS NEW <manufacturer> <product>

The Magnuson-Moss Act (Public Law 93-637) does not require any seller or manufacturer of a consumer product to give a written warranty. It does provide that if a written warranty is given, it must be designated as "limited" or as "full" and sets minimum standards for a "full" warranty.

<manufacturer> has elected not to provide any written warranty either "limited" or "full", rather than to attempt to comply with the provisions of the Magnuson-Moss Act and the regulations issued thereunder.

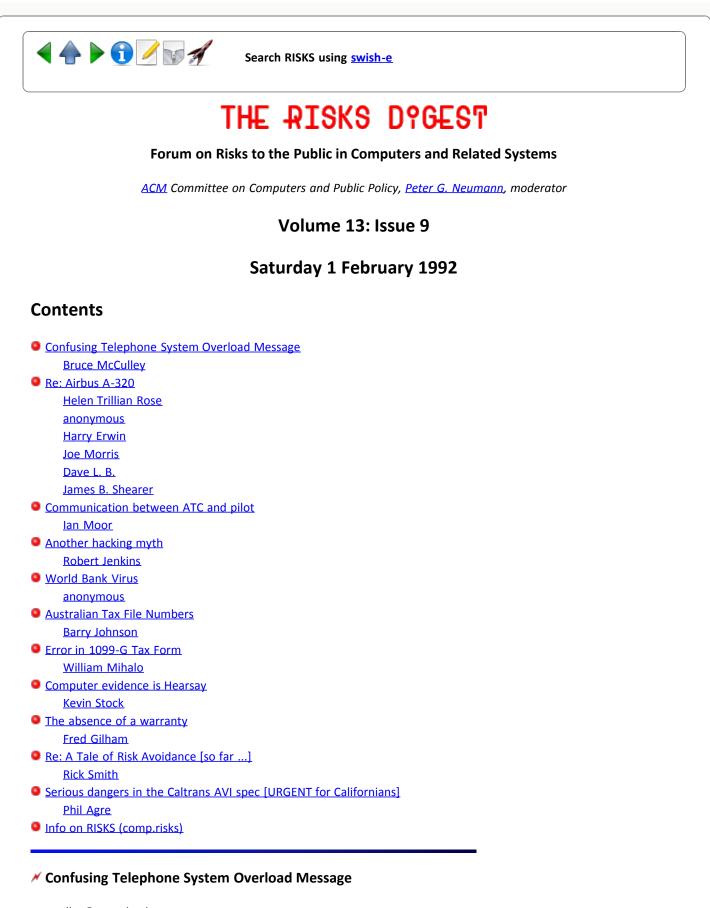
There are certain implied warranties under state law with respect to sales of consumer goods. As the extent and interpretation of these implied warranties varies from state to state, you should refer to your state statutes.

<manufacturer> wishes to assure its customers of its continued interest in providing service to owners of



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<mcculley@racy.zko.dec.com> Thu, 30 Jan 92 11:51:03 -0500 On Tuesday night (1/29/92), after President Bush's State of the Union address I happened to tune into the CBS television network as they were announcing a novel poll. They claimed nothing like it had ever been attempted before, and it sounded interesting so we stayed with them for awhile, and even tried to participate.

The basis for the poll was an interactive telephone system set up at a site in Omaha, Nebraska, with an (800) WATS line to allow toll-free access from anywhere in the US. Early in the show CBS announcer Charles Kuralt reported that the telecommunications center was capable of handling thousands of calls per minute, "so there should be no problem". HA!

Participation required a touch-tone phone, so that callers could respond via keypad entry to the canned questions posed by the automated response system. Although we live in a rural area with old mechanical switch gear, my phones all can switch between rotary and touchtone mode, so I could dial up using pulse mode and then switch to tone for the response.

After watching a few minutes to see what additional explanations were given, I decided to try accessing the poll. At the time they seemed to be running at a couple of thousand calls per minute. My initial attempt to call them resulted in a very long dead interval, followed by a message saying "Your call cannot be completed as dialed, you must supply more digits in the number dialed."

That seemed strange, so I tried redialing several times, more carefully, with similar results. Since the map showing calls received was showing nothing from our area of New England (New Hampshire and Maine were both showing null), I wondered if there was a problem with the WATS routing or something, that might have caused the strange error message. So I called the operator, and when I started to say I was having trouble dialing an (800) number she immediately asked if it was the one that had been given on TV. When I said it was, I was told that the lines were flooded.

Apparently the volume of calls was either forcing the long-distance system into some strange failure mode in which it thought more digits were required in the number being called, or there was a mismatch between the particular error condition and the error message being used. I suspect, based on my limited knowledge of the telephone network, that there may have been some timeout or connection loss or contention or something that inadvertently truncated the routing information string, due to the huge volume of calls.

Shortly afterward, with the display showing about 125,000 calls processed, Dan Rather reported on the air that AT&T was estimating there had been about 7,000,000 call attempts! Obviously their throughput was a little below the capacity requirements...

BTW, using redial, I was able to access the number on a subsequent attempt, and did get my response included in the poll. At that time they were reporting about a hundred thousand calls processed. From the ratio of call attempts reported by AT&T to calls processed it looked to me like the ratio was upwards of 70 to 1. It took me only about ten tries or so, so I guess I was lucky.

The risk seems obvious, experimenting with a novel application in a live production environment requires some careful system analysis and planning to

avoid unexpected errors.

One thing I'm curious about, wonder what their phone bill was? --bruce mcculley

### ✓ Speculation on latest A-320 crash: why? (Joel Upchurch, <u>RISKS-13.08</u>)

Helen Trillian Rose <hrose@eff.org> Tue, 28 Jan 1992 23:31:25 -0500

Joel> It might be informative to compare the A-320 accident rates to Joel> other planes that have a two man crew, rather than comparing it Joel> to planes of similar size that use a three man crew.

OK. We'll do this.

The Boeing 757. No total hull losses. No incidents \*at all\*, that I can recall.

The Boeing 767. One total hull loss, due to a problem with the engines (and on the engines that were least used. The ones in question were the Pratt & Whitney, while most customers had the GE/SNECMA).

The Boeing 747-400 (though not a 2-engine plane, is the most "technologically advanced", aside of the A320, with an almost total glass-cockpit) some incidents, but no hull losses. The 747-400 is particularly interesting because earlier models had three flight crew members.

The A-320 is about the same vintage as the 747-400, and is newer than the 757 and 767 by a good five plus years.

Helen Trillian Rose <hrose@eff.org> EFF Systems and Networks Admin

## **#** A320 crash may have been caused by ATC/Pilot miscommunication

<[anonymous]> Tue, 28 Jan 92 12:33:32 XXT

... The AT320's fly-by-wire system or glass cockpit ... may not have been directly involved in the lastest A320 crash.

A U.S. air safety source informs me that initial information suggests that a miscommunication between Air Traffic Control and the A320's pilot may have been the primary cause of the accident. Apparently the A320 was originally on a landing path to a runway with a fairly rapid descent slope. Sometime fairly late in the landing sequence, the pilot was ordered to a different runway by ATC, but may not have been warned that the new runway would require a different descent to avoid slamming into a mountain. The pilot descended at the original rate and the crash resulted.

Before someone argues that the automated information transmission systems being planned would have solved this problem, it's worth noting that many are very

concerned that such information systems would deprive pilots of information being sent to other planes, which they might need to know to avoid collisions or other problems. Many accidents have been avoided by pilots who heard ATC directions being given to \*other\* pilots (over conventional radios, of course) and realized that they themselves needed to take evasive action!

#### Ke: Speculation on latest A-320 crash: why?

Harry Erwin <trwacs!erwin@uunet.uu.net> 29 Jan 92 13:25:27 GMT

There is an old story about WWII in the Pacific, where an operations research team was sent to the combat zone to determine where armor should be added to the fighters in use. Originally they were going to survey aircraft returning with battle damage to see where the battle damage was concentrated--the armor was to be added to those areas. However, an older analyst pointed out that the armor should be added where there was no battle damage--planes receiving damage in those areas were not returning.

Harry Erwin erwin@trwacs.fp.trw.com

#### Ke: Another A-320 crash in France (Bennett, <u>RISKS-13.06</u>)

Joe Morris <jcmorris@mwunix.mitre.org> Thu, 30 Jan 92 11:09:24 -0500

>In <u>RISKS 13.05</u> Romain Kroes, Secretary General of SPAC is quoted as saying >"...it has been clear to us that the crews were caught out by cockpit layout" >

Surely this statement implies that there is a problem with training
 rather than the software or the crew

Not necessarily. Especially in stressful environments, a poorly-designed cockpit layout can be a disaster waiting to happen.

An aviation example on a smaller scale is the control panel layout of the flight instruments. For years there was no standardization of what instrument went where, neither between manufacturers or even between models. Only after studies showed that there was a quite significant safety advantage did the designers agree to the "basic" formation:

airspeed	artificial	altimeter
indicator	horizon	
turn-and-	gyro	vertical speed
bank indicator	compas	s indicator

Prior to the standardization these instruments could be almost anywhere in the cockpit. (Of course, we now have the interesting problem of trying to figure out how to best present the information on integrated displays in an EFIS (Electronic Flight Information System) environment.)

Another example of poor cockpit design was the way that Beech Aircraft moved cockpit controls around in different years in some of its airplanes. In some years the Beech Bonanza airplane put the control for the wing flaps (which are to be retracted after landing) on the left side of the cockpit and the gear retraction switch on the right; in other years the positions were reversed...with the obvious problem of pilots retracting the landing gear while on the ground. Beech also had a disconcerting habit of not following common industry practice in the order of the engine controls: where most designers put the controls on the panel in left-to-right sequence of throttle/prop/mixture, some Beech products used throttle/mixture/prop.

My point is that while training can teach a pilot about the particular idiosyncrasies (or idiotsyncrasies) of a particular airplane, a design which is nonstandard and/or unintuitive and/or misleading can be the trigger for failures which are eventually blamed on "pilot error".

This does have a direct significance to the normal subject matter of the RISKS-FORUM: the design of user interfaces in software systems. In fact, it's almost exactly the same issue: poorly-designed, or nonstandard, or "slightly" different interfaces between programs which perform similar functions are one of the reasons for many of the problems we have in this industry.

Joe Morris

#### 🗡 A320 Crash

<dlb@osf.org> Sat, 1 Feb 92 15:53:12 GMT-0400

A couple of comments about topics related to the A320 crash:

Potential of the FAA banning or restricting the A320 for nontechnical reasons (i.e. politics or advantage to US aircraft manufacturers): I think this is unlikely for at least two reasons. First, at least one major US airline (Northwest) has a significant A320 fleet. There may be others. If anything, the FAA is more beholden to US airlines than it is to US aircraft manufacturers. Second, the FAA is has an excellent reputation in safety matters to consider/defend. Aviation authorities in many other countries look to the FAA on aircraft safety matters, and routinely implement FAA safety directives. Issuing an unjustified safety directive with significant impact would do major damage to the FAA's status, influence, reputation, etc.

2-man crew (vs. 3-man) as a major factor. Highly unlikely. Virtually all recently manufactured aircraft (newer 737's, 757's, 767's, 747-400's, MD-80, MD-11, ... [hope this list is correct]) have two man crews. None of them have the crash record of the A320.

On the other hand, I wonder if we're looking at the wrong statistics. Fatal aircraft crashes are so few and far between that it's hard (statistically) to draw reliable inferences from such spotty data. I'd be much more comfortable looking at data that included significant failures that could have caused the aircraft to crash (but the plane didn't due to skill of the crew, luck, etc.).

I'm sure the FAA keeps such numbers, but of course they're not newsworthy because nobody died, and there aren't any good pictures ...

--Dave

#### 🗡 3 man aircrews

<jbs@watson.ibm.com> Thu, 30 Jan 92 18:33:31 EST

Joel Upchurch suggests 3 man aircrews will be safer than 2 man crews. Studies have shown 1 man police squad cars are safer than 2 man squad cars. Nevertheless police feel safer in 2 man cars (which may be part of the problem). I suspect something similar may be true of aircrews.

James B. Shearer

#### Communication between ATC and pilot

<iwm@doc.imperial.ac.uk> Wed, 29 Jan 92 19:35:55 +0000

Communication between Air Traffic Control and Pilots is currently verbal and in English (as a `Universal' language).

An item in a recent BBC radio program mentioned work on a possible replacement. They played back a recording of a dialogue where neither participant had English as a first language as a demonstration of misunderstandings that happen. The cure was to be a means of transmitting coded messages, presumably displayed in the pilot's native language, and presumably vice-versa. The interviewer asked `why not have the commands transmitted directly to the plane?', and was reassured that the pilot would have ultimate control.

However nothing was said about:

Error checking, natural language is redundant, but coded messages may not be.

What happens if the message to be sent was not anticipated by the system designer (Elephant on runway ?).

How the message was displayed: Headup display, voice, or another console display

lan Moor

### Another hacking myth

Robert Jenkins <rjenkins@cix.compulink.co.uk> Fri, 31 Jan 92 20:35 GMT

There has been an instructive little flurry about hacking in the British press.

It starts with Police Review, 17 January 1992: A columnist, C H Rolph, writes: "Did you know that there are hackers (i.e., people who make a hobby out of studying and programming other people's computers, or who get unauthorised access to computer systems by telephone) making a good living out of `cleaning up' people's driving licences. A wealthy man with an endorsed licence will pay a lot to have his file beautified at the Driver and Vehicle Licensing Centre at Swansea. I'm told that for 100 pounds a point, it is possible to get an endorsement completely erased, and then apply for and get an unblemished licence. Or was, until fairly recently."

The Times took up this "revelation" and, on 20 January, reported that "an investigation is under way after claims that computer hackers are wiping motorists' penalty points from the DVLC computer in Swansea. The hackers are charging 100 pounds for each penalty point, according to the Police Review".

On 31 January, C H Rolph returned to the affair. He referred to the Times story and said "I didn't quite say that. I said there were allegations that this \*had been\* going on. And it turns about that there had certainly been attempts. The Driver and Vehicle Licencing Centre at Swansea tells me that the story first appeared in the \*Sun\* in 1986, and that it was at once jointly investigated and refuted by the DVLA and Scotland Yard ... "

Looks like pretty bad behaviour by C H Rolph (a former senior police officer, by the way). His original story seems to have had no foundation whatsoever (the \*Sun\* is not a serious newspaper), but he is trying to wriggle out of accepting fault. And the Times doesn't come out of it well, either. Doesn't \*anyone\* check out hacking stories, or do journalists prefer urban myth. (I write as a journ.)

[This sounds as if an old tale had been warmed over. See <u>RISKS-2.38</u>, 8 April 1986, for Brian Randell's contributed item on the alleged DVLC hacking activities. (See also Software Engineering Notes, vol 11, no 2, April 1986, page 4. [The reference is WRONG in the RISKS INDEX, which appears once again in the January 1992 issue of SEN, pp. 23-32. I just noticed that in digging for the original.) PGN]

### 🗡 World Bank Virus

#### <[anonymous]> Recently

The bit about the World Bank virus [Ted Lee, <u>RISKS-12.36</u>, and Software Engineering Notes, Vol. 16 No. 4 (Oct. 1991) p.17] was actually a bit overblown. A few dozen networked PCs did get hit, but it was just one of those things that came off a diskette of questionable origin. There was no `international army of nerds and police experts' required to track it down, although it did occupy internal staff for several days to clean it out. Apparently the Bank's efforts to have Time print a correction came to naught.

### 🗡 Australian Tax File Numbers

## BARRY JOHNSON <WB15471@ibrdvax1.bitnet> Wed, 29 Jan 92 10:12:00 EST

Reading the January 1992 `Inside Risks' column in the CACM reminded me of what seems a very relevant article in "The Australian Computer Journal", Vol. 22 No. 1 (February, 1990) pp. 11-20 [published by the Australian Computer Society (ACS)]: 'Implications of the tax file number legislation for computer professionals'. After years of public resistance against anything like a Social Security Number, the Australian Government finally opted for a 'tax file number.' Although organisations such as employers and banks are expected to collect this number so that it can be included when submitting information to the federal tax authorities, there are also VERY strong legislative safeguards:

- It can ONLY be used for tax-related functions.
- It must NOT be disclosed to anyone who does not need, nor revealed if not immediately relevant.
- It may NOT be used as a national identification scheme nor for building up a database on individuals nor for matching personal information.

After discussing the meaning and implications of the legislation, the article touches on implementation issues (access control, personnel screening, communications and operating system security, and professional responsibility) that relate to the securing of the number. It discusses in some detail the choices of including the tax file number in a file/table with other personal information versus isolating it in a separate file/table. Interestingly, the article opens by noting that the legislation is based on privacy principals espoused by the Organization for Economic Cooperation and Development (OECD). It might be interesting to know what they are exactly ... If you would like a copy of the article and are unable to get it from anywhere else, I would be glad to send a copy if you can provide an address. Regards ... BJ

#### 🗡 Error in 1099-G Tax Form

William Mihalo <wmihalo@lucpul.it.luc.edu> Wed, 29 Jan 92 12:12:53 -0600

Last week I received an erroneous form 1099-G from the state of Indiana. The form erroneously claimed that I had received a large tax refund from the state. A call to the local state revenue office revealed that a faulty computer algorithm had created the problem. Apparently, if you claimed a tax refund or received a tax deduction, and also filed an estimated tax payment for the first quarter in 1991, the algorithm >added< the two numbers together rather than subtracting one from the other.

In my case, the error was compounded by a combination of a misplaced decimal point and adding the numbers together. The tax rate for Indiana is 0.034. Thus if you have a \$1,000 tax deduction, it reduces your tax liability by \$34. The statement that I received had apparently used 0.34 as the tax rate and added this to the amount owed and estimated taxes.

The person at the state revenue office said one million people were affected by the error. But I'm not certain if it's that large. At any rate, don't people

bother to check their software for mistakes before doing a mass mailing? The last time I received an erroneous 1099 form, I underwent three audits for three years in a row before the IRS finally recognized the error.

William E. Mihalo

#### Computer evidence is Hearsay

Compta) Wed, 29 Jan 92 09:44:38 GMT

[ Unfortunately I don't have a citable source for this as I no longer live in the UK and so I rely on BBC Radio for this news. ]

Local taxes in the UK were changed a couple of years ago from a system known as the "Rates", which was based on property values, to a system called the "Community Charge" (by the Government; most people call it the "Poll Tax") which is based on the number of adults living at an address. Many people consider the new system unfair, and a campaigning movement has been set up to fight against it.

One of the principal attacks has been simply refusing to pay the demands. Local councils have therefore taken defaulters to court to request orders for payment. However, the magistrates' courts which should deal with such cases are refusing to hear them, on the grounds that computer output is hearsay and therefore not acceptable as evidence.

[ Curiously, in the main criminal courts, computer evidence is acceptable as a result of specific legislation, but this legislation does not apply to the lower courts. The government has promised to end this anomaly. ] Kevin Stock

### The absence of a warranty

Fred Gilham <quail@csl.sri.com> Tue, 28 Jan 92 18:57:32 PST

My understanding is that if a warranty is not provided, the implied warranty gives the buyer quite a bit of protection. Manufacturers supply `limited' warranties for the very reason of saying how far they are willing to go, and for how long, to remedy a problem with their product.

An implied warranty, as I understand it, usually says something to the effect that the thing is supposed to perform as advertised or specified in instructions that come with it, basically forever.

So, if the manufacturer doesn't supply a warranty, the product had better be good.

-Fred Gilham

# **K** Re: A Tale of Risk Avoidance [so far ...] (Thorson, RISKS-13.08)

Rick Smith <smith@SCTC.COM> Wed, 29 Jan 92 13:18:21 CST

Mark Thorson (mmm@cup.portal.com) responded to a posting by "Kai-Mikael J\d\d-Aro" <kai@nada.kth.se> in <u>RISKS DIGEST 13.05</u>:

>Tools will always be pushed to their limit, because the limit is actually in >the programmer and it is the fundamental nature of programmers ...

>Will Kai-Mikael J\d\d-Aro find himself next year creating state diagrams
>with the complexity of a street map of Stockholm ... ?
>This might open a whole new range of computer applications ... but there
>is no reason to believe these systems will be more reliable than the
>smaller systems built before the tool was developed.

We have 2 different classes of tools here, very different. As Mark said, the shift to (more) automatic programming simply abstracts away certain technical details in software development. This makes bigger problems easier to tackle, but that's not the essential value of formal methods.

I remember Kai-Mikael saying that his workbench provided tests of various state machine properties; this goes far beyond the rudimentary correctness tests a compiler might apply (eg type consistency). Thus, the formal methods \_do\_ give us more reason to believe in the system's correctness.

If the tool in question simply provides a graphic representation for some network (streets, whatever) then it isn't contributing much to increased software reliability. After all, the network's correctness would still depend on whether the coder sees any errors in it when it is created and manually reviewed.

Rick Smith. smith@sctc.com Arden Hills, Minnesota

## ✓ Serious dangers in the Caltrans AVI spec [URGENT for Californians]

## Phil Agre <pagre@weber.ucsd.edu> Thu, 30 Jan 92 14:06:58 pst

I just received the latest revisions to the State of California's proposed spec for automatic vehicle identification (AVI) equipment. This is the box that the state envisages attaching to your car that broadcasts your car's vehicle identification number (VIN) when pinged by a roadsite transmitter. The spec is being developed on the instructions of the state legislature, which is considering automated systems for collecting tolls. The spec has been through a number of revisions. The latest, dated 17 January 1992, is considerably different from the others. It is an irritating document because so little is explained about how toll collection would actually work, and in particular whether it would be necessary for every car on the road to have one of these transmitters. Many of the new revisions are highly technical in nature, but some RISKS-relevant trends are clear. First and most obviously, the proposal no longer contains any language at all about privacy or about encryption. Previous drafts had specified the use of DES, but this is gone. In the former sentence "The initial data records are designed for voluntary implementations of automatic toll collection, where security and anonymity are not overriding concerns.", the phrase "where ... concerns." has now been struck (section 1702.1). Whereas the former document had provided both encrypted and unencrypted versions of the "reader communications protocol" (section 1704.5), the encrypted version is now gone.

But this seems to be a symptom of a much deeper change in the purpose of this whole spec. Caltrans (the state Dept of Transportation) has generalized the proposal; the "AVI" equipment is no longer specifically aimed at toll collection but is now intended to support a much wider range of applications. For example, in section 1701 "Definition[s]", the term "Transponders" has been changed from "Electronic devices attached to a vehicle and contain information which can be communicated to the reader." to "Electronic devices that contain information which can be communicated to the reader." New text in section 1702.1, "Objectives", reads "It is further envisioned that more complex data records will be developed to handle anonymous transactions, secure funds transfers, information transfers, and other transactions between the Reader and the Transponder that will be defined as needed." Caltrans will authorize new record types, but "shall pass this responsibility to an appropriate standards setting organization when one is established and recognized."

It seems to me that this is a serious situation, for two reasons. The first reason is narrow and clear: the state is about to receive an AVI spec that calls for an unencrypted protocol for toll-collection purposes. This is a serious matter in any case, but just how serious depends on whether it will be compulsory to attach one of these boxes to your car. I cannot understand how automatic toll collection could work unless every car has a transponder. (Maybe there's a box that can "see" a car going by, like the European boxes that issue speeding tickets automatically, and then determine whether any of those cars failed to transmit their VIN's? Even this is a scary enough thought.) The spec certainly reflects no effort to develop a proposal that would not require cars to transmit their VIN's, say through public-key encryption or the anonymous purchase of a transponder that gets decremented like a phone-card.

The broader and murkier reason for worry is that the state is envisioning a bureaucratic mechanism for the multiplying applications of automatic tracking mechanisms. The spec is actually broad enough, in principle anyway, to encompass certain kinds of anonymous schemes (as section 1702.1, quoted above, mentions), but the proposal reflects no analysis of the specific technical requirements of anonymous schemes. In effect, all of the hard social issues have been pushed down the line, to the committee that will authorize new uses of these boxes. Once the boxes exist and are in wide use, though, that will be a whole new ball game. We ought to stop now and think. Do we want to set up a bureaucratic mechanism that can turn out automatic tracking schemes on an assembly-line basis, hoping that we can hold the line on privacy and other civil liberties by keeping careful enough track of this process?

Or should we take some action -- for example, writing letters to the Pete Wilson, the state legislature, and Caltrans -- to get this entire process to be suspended long enough for a proper public debate? I vote for the latter.

The official address for public commentary is as follows ("All written comments received by February 6, 1992, which pertain to the indicated changes will be reviewed and responded to by the Department as part of the compilation of the rule-making file."):

Les Kubel, Chief Office of Electrical and Electronics Engineering Department of New Technology, Materials and Research PO Box 19128 Sacramento, California 95819-0128

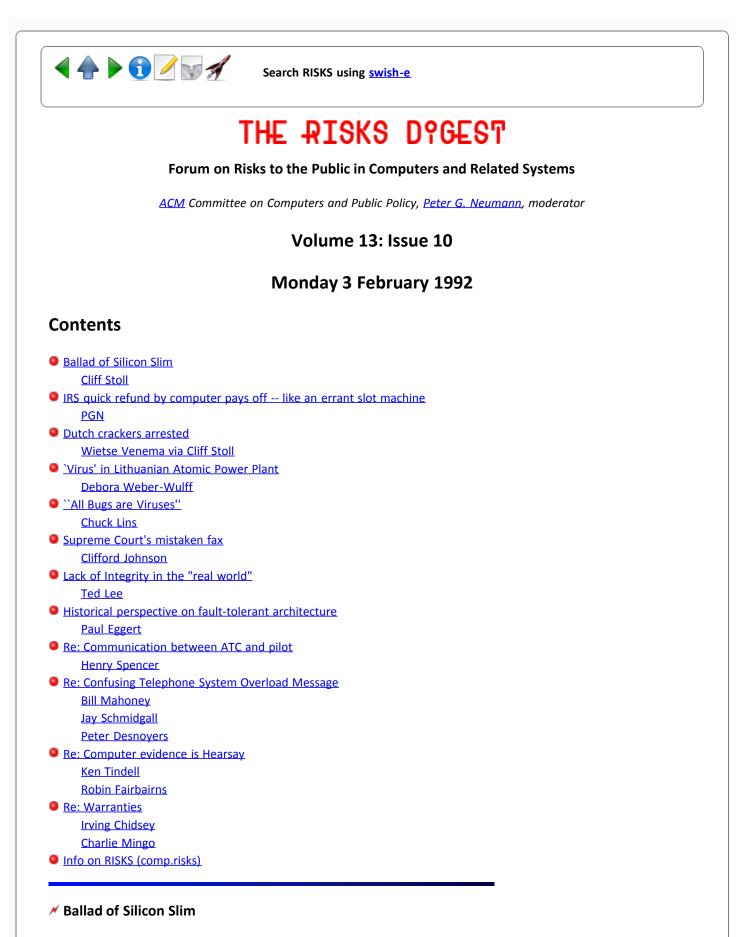
More importantly, we need to publicize the issue, so that Californians -- and others who live in jurisdictions that might adopt the California proposal as a model -- can make an informed choice.

Phil Agre, UCSD



Search RISKS using swish-e

Report problems with the web pages to the maintainer



## Cliff Stoll <stoll@ocf.Berkeley.EDU> Mon, 3 Feb 92 00:53:37 -0800

Dr. Demento collects the weirder songs for his nationally syndicated show -he's one of the best reasons to own a radio. Last week's program featured The Ballad of Silicon Slim, a country & western song by John Forster.

It's about a rootin-tootin, home computin' guy who breaks into Chase Manhattan Bank and snags a penny from everyone's account. This salami-slicing thief makes millions, gets caught, tossed in jail, but is popped out by a computer.

It's a song praising the thief as being democratic (stealing equally from everyone), and carries several dubious stereotypes (the best programmers break into computers, outsiders are the biggest threat to banking systems, skimming of bank accounts won't be noticed).

A ballad about a computing thief. Had to happen sometime!

-Cliff Stoll stoll@ocf.berkeley.edu

A few excerpts (without permission of copyright holder; I'm trying to reach him)

In the dead of night he'd access each depositor's account And from each of them he'd siphon off the teeniest amount. And since no one ever noticed that there'd even been a crime He stole forty million dollars -- a penny at a time!

Little Janet was only eight but she had her own account And the seven dollars in it was to her a huge amount. So the day that penny vanished one unhappy little tot Screamed, "Hey, what happened to my penny?" And the teller tried to tell her but could not.

Is your whole year's withholding getting to the government? Have you figured out your FICA to the hundredth of a cent? Though the average Joe don't even know how much his FICA was Out there, somewhere, there's a software packin' buckeroo who does!

## IRS quick refund by computer pays off -- like an errant slot machine

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 3 Feb 92 17:34:40 PST

If you were one of the 1.1 million people who filed a 1991 tax return electronically between 10Jan1992 and 27Jan1992, you may have gotten a notification that a refund was forthcoming even if one was not. Apparently during that period the IRS computer program ignored all back-tax debts, which would otherwise have offset the refunds. Relying on the refund notification, lenders have been making loans that were (supposedly) secured by the expected refunds. No one knows yet how many such unsecure loans were actually granted. [Source: San Francisco Chronicle, 3Feb1992, p.A3, from the Washington Post]

### Dutch crackers arrested

Wietse Venema <wietse@wzv.win.tue.nl> [missing, BUT BEFORE 3 Feb 92 01:03:32 -0800]

> reposted from alt.security and forwarded to Risks by Cliff Stoll <stoll@ocf.Berkeley.EDU> [and lightly edited by PGN]

This is a revision of an earlier posting carrying the same title. Any inaccuracies are my own responsibility.

According to Dutch TV and newspaper reports, the Amsterdam police have arrested two computer crackers and seized their equipment. A press conference was held on Friday 31st. The two made a full confession.

The reports state that over the past four months, R.J.N., age 25, computing science engineer, and H.W., age 21, c.s. student, installed so-called Trojan horses on a computer system of the Amsterdam Free University, and used that same system to break into computer systems in the US, Canada, and several European countries. According to a Dutch police spokesman, the two had no intention to damage or to steal information, but were doing it `just for kicks'.

Dutch law on computer crime is still in preparation. Apparently, the charges are based on existing law: falsification (corrupting systems files in order to get privileges), destruction of property (rendering a computer system unusable), and fraud (using stolen passwords).

Both fidelio and wave were students at my faculty, so I know them personally. The sad thing is, had the police been ready for this type of action a year earlier, they would probably still be free.

Wietse Venema, dept. of Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands

#### Virus' in Lithuanian Atomic Power Plant

Debora Weber-Wulff <weberwu@inf.fu-berlin.de> Mon, 3 Feb 1992 07:40:17 GMT

"Berliner Zeitung", 3Feb1992 ([East] Berlin), translated by DWW.

"Sabotage fails - Virus in Power Plant Program for the Lithuanian Atomic Power Plant in Ignalina vaccinated

Vilna/Moscow (dpa)

This past weekend an act of sabotage against the computer system for the atomic power plant in Ignalina failed. A worker in the computer center of the plant tried on Thursday to plant a virus in a program in the non-nuclear part of the reactor, in order to cause disruption. dpa learned on Saturday from Vilna that the man probably wanted to get money from the reactor managers for repairing the damage he himself causes. The plant engineers managed, however, to repair the damage themselves in a very short time, according to information from the news agency ITAR-TASS, which is based on information from the government press office in Lithuania. A warrant for the arrest of the sabotager has been issued, and officials state that he will be prosecuted.

The shutdown of one of the two reactors since Thursday has nothing whatsoever to do with the attempted sabotage, said the deputy Lithuanian energy minister, Saulus Kutas. ["Wer das glaubt, wird seelig." LOOSELY TRANSLATED AS "If you believe that, you'll believe anything." dww]

[And goes on to explain about the tiny leak in the cooling system and how the water is not radioactive, and there are no problems, and a team of Swedish specialists looked at the reactor and found no big problems, but they do have a list of 20 little things they want to look at, and the Swedish government is going to pay for it all.]"

Debora Weber-Wulff, Institut fuer Informatik, Nestorstr. 8-9, D-W-1000 Berlin 31 +49 30 89691 124 dww@inf.fu-berlin.de

### ``All Bugs are Viruses''

"Chuck Lins" <chuck\_lins2@gateway.qm.apple.com> 3 Feb 92 15:01:23 U

While having dinner I overheard two automobile mechanics discussing a problem one had with one of the fancy automotive diagnostic systems. Apparently, any attempt to 'take a measurement' caused a catastrophic failure in the system (i.e., it 'crashed'). The cause was attributed to a `virus'. While to a computing professional such rationale appears ludicrous, it is quite a logical conclusion for the layperson.

Chuck Lins, lins@apple.com

## 🗡 Supreme Court's mistaken fax

"Clifford Johnson" <Cliff@Forsythe.Stanford.EDU> Mon, 3 Feb 92 12:03:51 PST

From a UPI press release:

The Supreme Court's decree topped a roller-coaster day for refugees waiting to learn their fate. Earlier Friday, the clerk's office of the 11th Circuit issued an order allowing the government to send the refugees back to Haiti. But 4 1/2 hours later, it said that order had been made by mistake. ``It was a clerical error,'' said Joyce Larkin, deputy clerk. ``The order was erroneously issued. The motion filed by the government to stay the injunctive order issued by Judge Atkins remains pending before this court.'' Kembra Smith, motions attorney for the 11th Circuit, said a facsimile message between judges apparently was sent by mistake to the clerk's office, and the erroneous order was then issued. ``I

think we got an erroneous fax today, directed between the judges. It should not have come here -- it should not have been released," Smith said. She said there had been no final decision by the court, and that it should not be assumed that the court necessarily will issue an order similar to the one issued in error. "They (the clerk's office) received a number of documents after the office received that (erroneous fax)," she said. "A decision is probably in the near future. But there's no way to know that. Any time period is totally speculative on my part." Smith said the mistake was unusual -- and highly embarrassing to the court because of the magnitude of the case. "We're aware that it's fairly outrageous," she said. "Hopefully, this will never happen again. Oh my God, especially in a case like this."

[I can only add that had this been a last-day death penalty case, the error could have caused an unjust killing -- 4.5 hours is a long enough delay, and in a case involving less people, the delay may have been much greater. CJ]

#### ✓ Lack of Integrity in the "real world"

<TMPLee@DOCKMASTER.NCSC.MIL> Mon, 3 Feb 92 16:19 EST

There's been a fair amount of writing lately that the "real world" needs protection against loss of integrity, not loss of confidentiality. I'm not sure it even cares about that. Last week I learned something about how Hennepin County (where Minneapolis is located) handles important documents that sort of bothers me.

I needed to get a certified copy of a power of attorney that we had filed with the county's title registry a couple of years ago. I walked into a 30' x 30' room that had a clerk, a copying machine, a half dozen microfilm readers/printers and maybe half the room filled with racks of microfilm. A quite visible sign at the entrance said something like "please have the clerk retrieve printed documents; microfilm is self-service." Several lawyer-looking people appeared in fact to have done that -- they were sitting in front of the viewers just like one does at a public library. Not wanting to wade through the film I just gave the clerk the document number. She went over to the appropriate rack, got the film, and made a print of what I had asked for, which she then duly certified with the date and embossed county seal as being a true and accurate copy of the original that had been filed on such and such a date.

All true scam artists and system penetrators by now ought to be asking themselves the question that came to my mind as I drove home. After having done a little reconnaissance to find out what kind of film was used, what would have prevented me from going to view a film, pretend to re-file it, but actually slip it in my pocket and remove it? (I saw no signs of any alarms like they have in stores.) I could then take it to a lab and temporarily or permanently replace any image of a document with the image of one I had forged up on a laser printer. I'd return, put it back in the files, and then ask for a certified copy of the forged image. (I'd pick either a very recent document or a very old one so the chances of the film's being missed while it was being doctored would be slight.) I would think that if one could forge a legally-certified power of attorney giving himself power over, say, the affairs of the president of 3M, or perhaps, the deed to a downtown office building one could make a lot of mischief and probably a lot of money. (You'd have to be careful, but the possibilities are, as they say, intriguing.)

(Two additional points to note: nowhere was I asked for identification, although I did have to sign for the certified copy. Also, the registrar does NOT keep any originals -- all they have are the microfilm copies; we didn't have the original of what I needed because that had in fact to be deposited at a different state office.)

### Mistorical perspective on fault-tolerant architecture

Paul Eggert <eggert@bi.twinsun.com> Mon, 3 Feb 92 11:39:30 PST

I'd like to draw RISKS readers' attention to Daniel P Siewiorek's recent survey of fault tolerant computer design:

Daniel P Siewiorek, Architecture of Fault-Tolerant Computers: An Historical Perspective, Proceedings of the IEEE 79, 12 (Dec 1991), 1710-1734

Siewiorek proposes a 3D design space and classifies two dozen well known systems ranging from the Univac I to the Galileo mission. There's a wealth of juicy tidbits with a broad historical perspective. For example, I didn't know that the Univac I contained more error detection circuitry than most contemporary microprocessors -- the circuitry was essential because they couldn't simulate the machine in advance!

Although I highly recommend the survey, I have two reservations. First, publication delays have dated it a bit -- e.g. surely the new CM-5 deserves a place in Siewiorek's pantheon. Also, there's a frustrating lack of coverage of software fault tolerance, despite hints scattered throughout that software is a big problem area. Perhaps we'll have to wait for the book.

## Re: Communication between ATC and pilot

<henry@zoo.toronto.edu> Mon, 3 Feb 92 14:55:12 EST

> [direct message transmission from ATC to aircraft]

> How the message was displayed: Headup display, voice, or another console

> display

There was a piece in a recent Aviation Week (Jan 6, I think) on NASA experiments with a digital data-transmission system. The pilots who tried it generally liked it, with reservations. They wanted to see voice used during high-workload times like landing approaches, because they didn't want to have their heads down inside the cockpit reading a screen at such times. For communication at less busy times, though, they liked it a lot. Messages generally did not need repeating, which was needed for a significant fraction of voice messages. There was less room for misunderstanding, and more time to think about complex messages. Being able to scroll back and look at earlier messages was something they liked very much. They particularly liked digital transmission and scrolling back to earlier messages for weather data, since this gave them some sense of how weather was changing.

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

### Ke: Confusing Telephone System Overload Message (McCulley, <u>RISKS-13.09</u>)

Bill Mahoney <billzy@odin.unomaha.edu> Sun, 2 Feb 92 10:40:50 -0600

The Omaha World Herald reported that one problem with this level of calls is that quite a number of them went to an 800 number in Minnesota either by accident or because of other circumstances. The company in Minnesota is asking (unsuccessfully) for CBS to repay them for the several thousand phone calls that they received by accident, and is claiming that at least in some areas the phone number shown on the TV special was their 800 number and not the one for Call Interactive. CBS has decided that it should not have to pay for anyone dialing a wrong number (good point) and denies that the number shown on television was ever the incorrect one.

Bill Mahoney

#### Ke: Confusing Telephone System Overload Message

Jay Schmidgall <shmdgljd+@rchland.ibm.com> Mon, 3 Feb 1992 07:22:37 -0600 (CST)

... The owner of the store had been watching the SotU address and recognized his 1-800 number as the one CBS gave. He raced to the store only to find that his answering machine tape was filled to capacity (approx 50 msgs). He said some of the messages were pleasant, but others contained language unfit to print, apparently from frustrated viewers? He estimated the calls had cost him several hundred dollars in lost business. (No mention of any plans to sue CBS for compensation. :)

CBS also had some comments but I don't recall what those were; typical apologies for the screw-up and disbelief that it could occur come to mind, though. I don't recall any explanation being given for the screw-up.

In light of this article, I wonder how accurate CBS's numbers are:

> Shortly afterward, with the display showing about 125,000 calls
 > processed, Dan Rather reported on the air that AT&T was estimating there
 > had been about 7,000,000 call attempts! Obviously their throughput was
 > a little below the capacity requirements...

I can't seem to come up with an especially pithy RISK but perhaps our moderator can. To me, it seems either to be one of not very thorough testing of the system (I mean, c'mon, couldn't someone have \_dialed\_ the number before showing it to the entire nation) or perhaps a typical

transcription error, though as I said I don't recall any mention in the article.

-- jay

## ✓ Survey bias by equipment failure (McCulley, <u>RISKS-13.09</u>)

Peter Desnoyers <peterd@merlin.dev.cdx.mot.com> Mon, 3 Feb 92 11:54:04 -0500

A less obvious risk - although any phone-in survey is less than scientific, the low call completion rate (1 in 70) could further bias the results. Consider that the probability of success is probably strongly correlated with various factors such as geographic location (e.g. due to blocking systems that allow equal numbers of calls from areas with non-equal populations), population density (rural/urban/suburban), or ownership of a repeat-dial phone.

With an extremely high call-blocking probability, it is easy to imagine that these factors could result in a given population sub-group (e.g. residents of New Hampshire and Maine\*) being under- or over-represented in the sample by a factor of two or more.

Peter Desnoyers

\* I especially find it hard to believe that no residents of New Hampshire - who are supposed to live and breathe politics every 4 years, with a 70% presidential primary turnout - would have gotten through in the first few minutes if the blocking probability was uniform.

### Ke: Computer evidence is Hearsay (Stock, <u>RISKS-13.09</u>)

<ken@minster.york.ac.uk> 2 Feb 1992 13:55:39 GMT

>... However, the magistrates' courts which should deal with such cases are >refusing to hear them, on the grounds that computer output is hearsay and >therefore not acceptable as evidence.

It is a little more complex than this. The law regarding summoning non-payers requires that the Council send a bill (of course) and a reminder before any court action is possible. The computer evidence problem surrounds this. In the UK proof of posting in the Royal Mail is \_legally equivalent to proof of delivery\_ (a precedent was set in Victorian times - they had a better postal service then\*). Reams of computer printout are used to prove that bills and reminders have been sent, but all RISKS readers know that just because a computer prints out that a letter has been sent is no proof that is has. There have been a lot of software errors with Poll Tax systems (See RISKS passim) and I suspect that the Magistrates are so annoyed at having to deal with so many computer errors that they threw the cases out, which has now set a legal precedent.

Now, the Government has changed the law for the Poll Tax making computer evidence legal. There are worrying aspects to making computer evidence legal:

does the Plaintiff have to prove that the computer system is accurate? Or is it up to the Defendant to prove that it is full of errors? Will the accuracy of computer evidence ever be questioned? This problem will open up a whole can of worms in the English legal system, and I bet we will see non-computerate ill-advised legislators making sweeping changes which will create more problems than they solve. Sounds like a case for the EFF?

Ken Tindell \* I do not imply that the UK postal system is bad!

Computer Science Dept., York University, YO1 5DD UK ..!mcsun!uknet!minster!ken Internet: ken%minster.york.ac.uk@nsfnet-relay.ac.uk Tel.: +44-904-433244

## Ke: Computer (poll tax) evidence is hearsay (Stock, <u>RISKS-13.09</u>)

Robin Fairbairns <robin.fairbairns@lsl.co.uk> Mon, 03 Feb 1992 13:06:05 GMT

> [ Unfortunately I don't have a citable source for this as I no longer live

> in the UK and so I rely on BBC Radio for this news. ]

I had been surprised that no-one else had posted about this matter, and had dug out old newspapers: there were articles in `The Guardian' on Jan 16 and 17.

> [ Curiously, in the main criminal courts, computer evidence is acceptable as a
 > result of specific legislation, but this legislation does not apply to the

> lower courts. The government has promised to end this anomaly. ]

Actually, the case is a \_civil\_ one (presumably because the government never believed that the non-payment campaign would get off the ground). The specific legislation that Kevin talks about applies to Crown Courts and up for civil cases (I don't know what the rules are about criminal cases).

If there were only small numbers of defaulters, the ruling would presumably not be a problem: a council officer could attend the court for the (trivial) time it takes a magistrate to make an order. In fact, there were (until the ruling) hundreds of defaulters being dealt with in every court. All of this legal activity (and interest charges on loans to cover uncollected tax) is adding massively to the costs of administering local government. The (Labour Party) opposition has claimed that, on average, Poll Tax bills will go up by 50% in the coming financial year.

The government's promise to end the anomaly has not taken the form of `rushing legislation through'; the councils have complained that their collection strategy is in a shambles until the new legislation is passed.

## **Ke: Warranties (Hollombe, <u>RISKS-13.08</u>)**

Irving Chidsey <chidsey@smoke.brl.mil> 30 Jan 92 13:47:18 GMT

Jerry Hollombe questions the trend to selling things without

warranties. Does not the commercial code require that all things offered for sale be merchantable, unless the sellor limit this merchantability in some explicit way? That a program called Taxamatic-91 can be expected to compute my 1991 taxes correctly as long as I answer its questions correctly? That the sole purpose of a warranty is to limit the sellor's liability, and if there is no warranty, there is no limit. Therefore, if it is called Taxamatic, with no 91, and there is no mention of the year in the instructions, I have grounds for suit if it doesn't work correctly for my 92 taxes, and my 93 taxes, etc..

How can lack of a warranty be worse than one that says, more or less, "The sellor makes no claim that this product is error free, will operate correctly, or is merchantable."?

Irv Chidsey

#### Ke: The Absence of a Warranty (Gilham, <u>RISKS-13.09</u>)

Charlie Mingo <Charlie.Mingo@p0.f70.n109.z1.fidonet.org> 02 Feb 92 23:04:07

Under the Uniform Commercial Code, there are implied warranties, but they are much more limited than you suggest.

The basic implied warrenty is that of "merchantability" [UCC 2-314]; that is, the product is good enough to:

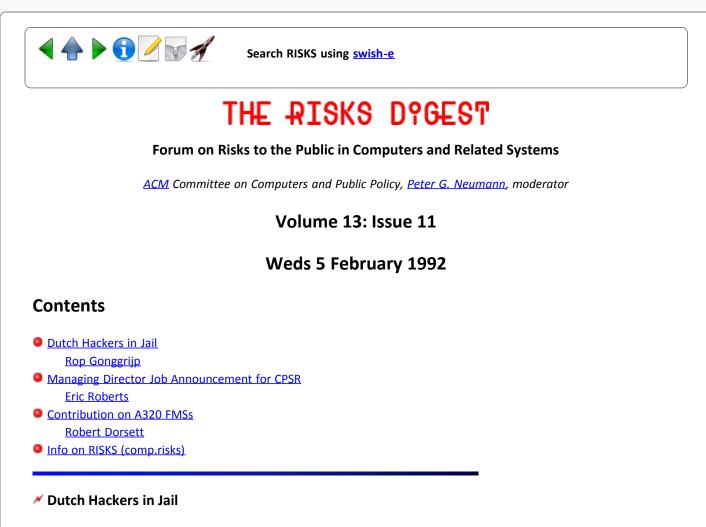
- pass without objection in the trade under the contract description; and
- in the case of fungible goods, are of fair average quality; and
- are fit for the ordinary purposes for which such goods are used; and
- run, within any agreed variations, of even kind, quality and quantity within each unit and among all units involved; and
- are adequately contained, packaged and labelled as the agreement may require; and
- conform to the promises or affirmations of fact made on the container or label if any.

There is also an "implied warranty of fitness for a particular purpose" when the merchant selects the product for the buyer based on a description of the intended purpose, and the buyer relys on the seller's skill and judgement. [UCC 2-315]

Neither of these warranties are perpetual; rather, they describe the condition the product is expected to be in when delivered to the buyer. The buyer has four years from the date of delivery to file a claim against the seller, regardless of when s/he becomes aware of the defect. [UCC 2-725]

Charlie Mingo mingo@well.sf.ca.us mingo@cup.portal.com Charlie.Mingo@p4218.f70.n109.z1.fidonet.org





Rop Gonggrijp <rop@hacktic.nl> 8 Feb 92 17:11:17 GMT

DUTCH POLICE ARRESTS HACKERS

The facts

At 10.30 in the morning of monday the 27th of January 1992 Dutch police searched the homes of two hackers. In the city of Roermond, the parental home of the 21-year old student H.W. was searched and in Nuenen the same happened to the parental home of R.N., a Computer Science engineer, age 25. Both were arrested and taken into custody. At both sites, members of the Amsterdam Police Pilot Team for computer crime were present, alongside local police officers and representatives of the national organisation CRI (Criminal Investigations Agency). Both suspects were transported to Amsterdam. The brother of one of the suspects was told the suspects could receive no visits or mail. All of this has happened more than one week ago and the two are still in jail as we write this.

#### The charges

A break-in supposedly occurred at the bronto.geo.vu.nl site at the VU University in Amsterdam. This UNIX system running on a SUN station (IP 130.37.64.3) has been taken off the net at least for the duration of the investigation. What happened to the actual hardware is unknown at this time.

The formal charges are: forgery, racketeering and vandalism. The police justifies the forgery part by claiming that files on the system have been changed. The vandalism charge is valid because the system had to be taken off the net for a period of time to investigate the extent of the damage. By pretending to be regular users or even system management the hackers committed racketeering, the police says.

Both suspects, according to the Dutch police, have made a full statement. According to a police spokesman the motive was "fanatical hobbyism". Spokesperson Slort for the CRI speaks of the "kick of seeing how far you can get".

#### `Damages'

According to J. Renkema, head of the geo-physics faculty at the VU, the university is considering filing a civil lawsuit against the suspects. "The system was contaminated because of their doing and had to be cleaned out. This cost months of labour and 50.000 guilders (about US\$ 30,000). Registered users pay for access to the system and these hackers did not. Result: tens of thousands of guilders in damages." Renkema also speaks of a `moral disadvantage': The university lost trust from other sites on the network. Renkema claims the university runs the risk of being expelled from some networks.

Renkema also claims the hackers were discovered almost immediately after the break-in and were monitored at all times. This means all the damages had occurred under the watchful eyes of the supervisors. All this time, no action was taken to kick the hackers off the system. According to Renkema all systems at the VU were protected according to guidelines as laid down by CERT and SurfNet BV (SurfNet is the company that runs most of the inter-university data-traffic in The Netherlands).

#### What really happened?

The charge of `adapting system-software' could mean that the hackers installed back-doors to secure access to the system or to the root level, even if passwords were changed. New versions of telnet, ftp, rlogin and other programs could have been compiled to log access to the networks.

What really happened is anybody's guess. One point is that even the CRI acknowledges that there were no `bad' intentions on the part of the hackers. They were there to look around and play with the networks.

#### About hacking in general

In the past we have warned that new laws against computer crime can only be used against hackers which are harmless. Against the real computer criminals a law is useless because they will probably remain untraceable. The CRI regularly goes on the record to say that hackers are not the top priority in computer crime investigation. It seems that hackers are an easy target when `something has to be done'.

And `something had to be done': The pressure from especially the U.S. to do something about the `hacking problem' was so huge that it would have been almost humiliating for the Dutch not to respond. It seems as if the arrests are mainly meant to ease the American fear of the overseas hacker-paradise.

#### A closer look at the charges and damages

The VU has launched the idea that system security on their system was only needed because of these two hackers. All costs made in relation to system security are billed to the two people that just happened to get in. For people that like to see hacking in terms of analogies: It is like walking into a building full of students, fooling around and then getting the bill for the new alarm-system that they had to install just for you.

Systems security is a normal part of the daily task of every system administrator. Not just because the system has to be protected from break-ins from the outside, but also because the users themselves need to be protected from each other. The `bronto' management has neglected some of their duties, and now they still have to secure their system. This is not damages done, it's work long overdue.

If restoring back-ups costs tens of thousands of guilders, something is terribly wrong at the VU. Every system manager that uses a legal copy of the operating system has a distribution version within easy reach.

`Month of tedious labour following the hackers around in the system'. It would have been much easier and cheaper to deny the hackers access to the system directly after they had been discovered. `Moral damages' by break-ins in other systems would have been small. The VU chose to call the police and trace the hackers. The costs of such an operation cannot be billed to the hackers.

Using forgery and racketeering makes one wonder if the OvJ (the District Attorney here) can come up with a better motive than `they did it for kicks'. If there is no monetary or material gain involved, it is questionable at best if these allegations will stand up in court.

As far as the vandalism goes: there have been numerous cases of system management overreacting in a case like this. A well trained system-manager can protect a system without making it inaccessible to normal users. Again: the hackers have to pay for the apparent incompetence of system management.

This does not mean that having hackers on your system can not be a pain. The Internet is a public network and if you cannot protect a system, you should not be on it. This is not just our statement, it is the written policy of many networking organisations. One more metaphor: It's like installing a new phone-switch that allows direct dial to all employees. If you get such a system, you will need to tell your employees not to be overly loose-lipped to strangers. It is not the callers fault if some people can be `hacked'. If you tie a cord to the lock and hang it out the mail-slot, people will pull it. If

these people do damages, you should prosecute them, but not for the costs of walking after them and doing your security right.

#### Consequences of a conviction

If these suspects are convicted, the VU makes a good chance of winning the civil case. Furthermore, this case is of interest to all other hackers in Holland. Their hobby is suddenly a crime and many hackers will cease to hack. Others will go `underground', which is not beneficial to the positive interaction between hackers and system management or the relative openness in the Dutch computer security world.

#### Public systems

If you are not a student at some big university or work for a large corporation, there is no real way for you to get on the Internet. As long as there is no way for some people to connect to the net, there will be people that hack their way in. Whether this is good or bad is besides the point. If there is no freedom to explore, some hackers will become the criminals that government wants them to be.

"Our system is perfectly secure !"

(and if you prove it's not, we'll have you put in jail)

Felipe Rodriquez (felipe@hacktic.nl) & Rop Gonggrijp (rop@hacktic.nl)

Rop Gonggrijp (rop@hacktic.nl), editor of| fax: +31 20 6900968Hack-Tic Magazine (only on paper, only in Dutch)| VMB: +31 20 6001480The best magazine for staying in touch with the| snail: Postbus 22953,the Techno-Underground. Mail to info@hacktic.nl| 1100 DL Amsterdam

#### Managing Director Job Announcement for CPSR

### Eric Roberts <eroberts@CS.Stanford.EDU> Tue, 4 Feb 1992 20:06:14 GMT

National nonprofit organization working on issues concerning the social implications of computing technology seeks managing director to assume responsibility for overall organizational administration. Responsibilities include management of administrative staff and volunteers; preparation of reports; membership development campaigns; financial management; coordination of CPSR offices and chapters; developing organizational materials; and strategic planning. Experience desired in similar positions. Strong communications skills required. Computer and budget experience strongly preferred. Commitment to the peaceful and productive use of technology. Position requires an active self-starter who wants to help develop an exciting organization. Located in Palo Alto, California. May include periodic travel. Salary \$32,000-\$38,000, with benefits, depending on experience. Send resume in confidence to

CPSR, Managing Director Position P.O. Box 717 Palo Alto, CA 94302-0717 (415) 322-3778 cpsr@csli.Stanford.EDU

### Contribution on A320 FMSs

Robert Dorsett <rdd@cactus.org> Mon, 3 Feb 92 21:45:25 CST

It's apparent that some people don't have a clear idea of how the A320's automation is set up. This has been a problem with net discussions for the past couple of years, but it's not getting any better. There have been numerous comments attributing what are clearly flight management problems to the electronic flight control system (FBW): given the notoriety of the A320 (and its FBW) in the academic community, it has been assumed that other problems are unique to it. Many are not.

Following is an attempt to explain what flight management on the A320 is, how it differs from FBW, and how it compares to other airplanes (such as the 757). Issues pertaining to the Strasbourg crash appear about 2/3 through. A glossary for the (necessary) alphabet soup follows at the end. Manufacturers each tend to use their own proprietary jargon; in light of that, I've tried to keep the discussion as generic as possible.

First, the physical concept of "autopilot" is obsolete on the A320. Instead, Airbus uses a "Flight Management and Guidance System" (FMGS). A more generic term for this is a flight management \*system\* (FMS). Note the emphasis on \*system\*.

An FMS is a way to accomplish four major goals:

- o Control the flight path of an airplane, in four dimensions, from takeoff to landing.
- o Make sure that this is done as profitably as possible.
- o Provide high-level services to flight displays and other systems.
- o Eliminate many of the "book-keeping" roles in the operations environment, traditionally performed by a flight engineer.

An FMS has many components, the most important of which are:

1. A Flight Management Computer (FMC). This does all the thinking. It derives data from many sources, such as air data computers. On the A320, many input services are partially integrated into the FMS proper. An A320 has two FMCs.

2. Inertial Reference System (IRS) units. These are what Inertial Navigation Systems (INSs) have evolved into; when combined with an FMC, they lead to more features, and are more reliable. They provide position information to the FMC. The FMC has the capability of automatically tuning in VORs and DMEs and verifying the aircraft location, thus correcting for en route precession error in the IRS. There are three IRSs on the A320.

3. A Control Data Unit (CDU). This lets the pilot enter a variety of abstract data, such as the flight number, what the intended route of flight is, preferred cruising altitudes, navaids and fixes to use, etc. The FMC is able to relate all this to an internal database of airports and navaids, and provide a number of convenient features. Using this--as well as features which amount to being a glorified performance calculator-- the pilot can sketch out a relatively profitable trip. There are normally two CDUs on the A320, one for each pilot.

As the first of many asides, at least one recent poster has implied that the FMS interface is similar to that of an INS, which it isn't. The pilot generally does not deal with lat/long numbers, so the potential for a KAL 007 sort of mismanagement is minimal: he deals with gate numbers and four-digit ICAO mnemonics for the airport at hand (but mistakes are still quite common). Some airlines have card readers that feed everything in automatically: the pilot need only verify the flight plan. This process, too, is different from the INS. The user does not normally view the navigation product of the FMS through lat/long readouts on the CDU. Instead, a navigation display shows a plan view of aircraft position, in a variety of scales and formats. The use of the CDU is required when any changes to various types of abstract data are made.

4. A Flight Control Unit (FCU). This is what confuses a lot of people. The FCU is where the autopilot interface used to be in older airplanes, such as the 747-200. It looks a lot like it as well. It is used for selecting short-term features of the FMS, especially heading hold, altitude capture, rate of descent, and autothrottle. The FCU's similarity to an old-fashioned autopilot interface is intentional, but, again, it's just an interface to the FMS. This concept is extended to other input devices in the cockpit. The frequency selectors on the radio panels, for instance, serve as user-friendly input mechanisms for the FMS.

Autopilots (until the advent of FMSs) traditionally have been structured around the pilot commanding short-term actions, which the autopilot then faithfully executed. This frees the pilot to adopt a more supervisory role: he can deal with ATC, systems, track weather better, etc. It is also generally less fatiguing than hand-flying. Airbus classifies traditional autopilot management as "selected" control.

FMSs also provide such short-term capability (via the FCU). But the FMS can be set to meet all the waypoints and clearance altitudes \*automatically\*, without any significant interaction needed from the pilots on the CDU or FCU. Airbus classifies this as "managed" control.

In effect, with a properly set-up FMS, the pilot can plan a flight from takeoff to landing. After lining up the airplane on the runway, he can just turn loose

the FMS, which then flies the airplane, requiring minimal crew interaction. The system can then take the airplane through a category III landing (700 feet runway visual range). Of course, air traffic control is rarely so obliging, so en route modifications must be made to the stored flight plan.

This is all done with the presumption that the FMS will figure out and use the absolutely cheapest way to fly the airplane. Even a 1% waste of fuel can cost an airline tens of millions of dollars a year. The main problem with "profitability" is that ATC is not geared to handle FMS-equipped airplanes, and its actions soak up a lot of the "saved" money. It is not clear whether this situation will change in our lifetimes.

FMSs are here to stay: but the design of interfaces are a major point of contention among many pilots. Mention "automation," and they don't think EICAS or FBW: they think FMS. While many features have been added at the hardware level in the last ten years, the CDU interface has changed hardly at all. A significant criticism--and the most persistent--is that, since any changes to an airplane's clearance (the route of flight ATC has approved for it) require changes to the internal flight plan, and since this requires use of the CDU, thus leading to a heads-down posture, safety can be affected: the pilots are not able to practice "see and avoid." In addition, it requires a SIGNIFICANT refocusing of one's attention and attitude, from flying the airplane, to dealing with an unfriendly user interface. It therefore helps put pilots even further out of the loop. This increases workload, but workload can increase even more in terminal environments, where frequent changes to clearances are common (a terminal environment is the airspace where aircraft are being routed to or from a nearby airport). Many airlines have restricted CDU use under 18,000'; still more under 10,000'. In such cases, the airplane is flown with the FCU, or, occasionally, even by hand (!).

Balanced against the CDU interface problem is the high degree of "situational awareness" the overall system provides, when one isn't fiddling with the CDU. The FMS provides a number of output services, including navigation information:, the FMCs are the heart of navigation services. One can therefore look at one's navigation display, and see a graphic spatial representation of heading, track (calculated path across the ground), nearby alternate airports, where one will be when one completes a climb or descent, what VORs the airplane is using, where the fixes are, etc. This sort of thing is pretty popular with pilots. But the quality of the derived data products is dependent on the quality of data in the system: thus, there's a tendency to try to keep as much of the display "valid" as possible, which lends to excessive CDU interaction.

On the issue of "authority," it is important to note that the pilot must explicitly requests FMS services. The FMS is "on" all the time; but it only \*controls\* the airplane when the pilot wants it. Whether executing a stored flight plan, or selecting short-term features, the PILOT holds the ultimate authority over the operation of the system. If, after the FMS is engaged, it performs unsatisfactorily, the pilot can just "click it off" (disengage it). There are at least three ways to accomplish this (a switch on the sidestick, buttons on the FCU, or, as a very rare last resort, a circuit breaker). After disengagement, the pilot simply flies "manual" (although "manual" in the A320 is still filtered by numerous computers, and still an artificial construct). The capacity to disconnect assumes the pilot is "in the loop," and is aware that a problem (whatever its cause) exists, to the point of applying corrective action in time. Cockpit interruptions, heads-down postures (CDU interaction or systems diagnostics), fatigue, or checklists can affect this capability. Another factor is the WILLINGNESS to disconnect: a significant problem is that pilots tend to wait too long before clicking off a system; they can become over-dependent on automation.

It is unlikely that faults in FMS design could logically migrate to the FBW computers, or vice versa, barring \*possibly\* a significant electrical system failure. There are elaborate safeguards to protect against completely off-the-wall instructions, but a more insidious, higher-level (but erroneous) command within parameters would simply be quietly executed by the receiving system. It is impossible, as one person recently suggested on sci.aeronautics, for the \*FBW\* to "freeze" the airplane into some arbitrary navigation maneuver, such as a holding pattern (that tale, repeated at least twice in the last couple of years, is taking on the form of an Urban Legend).

The important point to note about all of this is that the FMS has NOTHING WHATSOEVER TO DO WITH FLY-BY-WIRE. It is at least a couple of levels "higher," from the systems integration perspective, than the FBW service. FMSs are used in virtually all modern airliners, such as the 757, 767, 737, MD-11, MD-80, A310, A300-600, and, yes, the A320. Pick an airliner manufactured since 1982, and it'll probably have a cockpit designed around an FMS control concept, regardless of whether it has glass displays, FBW, or both.

Of particular interest, recently, has been the A320 FMSs "vertical navigation" functionality. In what follows, "autopilot" should be regarded as a synonym for "FCU," with the understanding that it's just a high-level interface to the FMS, using a subset of FMS features, and can be "clicked off."

A few people have been saying things like "altitude can't be set on the autopilot." That is incorrect. The A320's altitude selector is located on the right side of the FCU. Not only can the user set the altitude to fly, but can also set the rate of climb that the airplane should fly at in order to achieve it. The latter can be achieved three ways:

1. By pressing an "Expedite" button, located under the altitude-selector window. This will make the airplane reach the desired altitude as FAST as possible, using either maximum climb attitude and climb thrust, or flight-idle and maximum airspeed.

(With the following two modes, one can either select a capture altitude, or let the airplane fly "free." The distinguishing feature between the modes is a simple push-button.)

2. By simply dialing a value into the vertical-speed selector. For example, if one wishes to fly 3000 feet per minute up, the user just dials in 3000 fpm.

3. By flying a flight path angle (FPA). This is an angle the airplane's flight path will make with the ground. The intended use of this feature is rather obscure (other advanced aircraft do not support it), but apparently one application is for use in conjunction with nonprecision approaches to airports. A non-precision approach is one that does not include vertical guidance: the airplane is vectored in a manner such that it reaches a "final approach fix"

pointed in the right direction relative to some sort of navigation aid, then flies down to a minimum descent altitude. It then flies toward the airport until it sees it, and can land visually, or is compelled to try again (or divert to an alternate). An ILS, in comparison, provides vertical guidance from the final approach fix down to the ground, even in very marginal visibility. A normal ILS (or visual) approach angle is 3.0 degrees; a non-precision approach is too complex to categorize briefly. The point has to be made, though, that FPA is one of the strangest features in the A320: the airspace system isn't really set up to let the pilots use it effectively.

On the A320, in a rather dubious interface, the FPA mode and vertical-speed mode share the same selector. The way vertical speed is set is to dial in a TWO-digit number. So 30 = 3000 feet per minute up; -30 = 3000 fpm down. There is no additional feedback--like a couple of extra zeroes-- to indicate one's dialing in "3000." The SAME selector, and the SAME indicator, are used to set "flight path angle." So 30 would then equal a flight-path command of 3.0 degrees down. The difference between the two modes, as said before, is the push of a button, and an easy-to-overlook decimal point. The A320 uses a liquid-crystal display, with fixed numeric elements, to display all of the FCU indicators.

So, say one wishes to fly a 3.0 degree flight path. This is the normal slant range between a "final approach fix" and an airport. This would give one a descent from 700 to 900 feet per minute, and the computer would automatically adjust the aircraft's attitude to maintain a glide path, if the pilot lowers flaps, commands a change in airspeed, etc. But there's a clear potential for disaster if this mode is \*confused\* with "vertical speed" mode. How significant is this? If one is 3000' above the ground, and sets a 3.0 degree flight path, one would contact with the ground in four minutes. If one accidentally engages vertical speed mode, instead, one will contact in sixty seconds. All this is a tad bit simplified, to relate it to normal "straight-in" approach angles: the let-down portion of a non-precision approach would require an even steeper angle (4.0 degrees), with similar consequences should modes be confused.

I am interpreting union comments on the Strasbourg crash as suggesting this type of mode confusion may have contributed to the crash. In this case, the FPA mode may have been used in response to an enroute descent air traffic control clearance. When the airplane crashed, it was descending at some 2300' per second, according to one source. The angle of descent between the two transition points the airplane was cleared to fly was 2.28 degrees (from 9000' to 5000', over 19 statute (?) miles).

Similar theories about the FPA mode abounded after the Bangalore crash, but proved unfounded (instead, a more complex pattern of FMS mismanagement emerged). The British pilots' union, though, early on cited the poor interface as one that needed to be improved, in a report dated July 1988, a few months after the airplane was introduced into service:

"4.2. Glareshield Flight Control Unit. Despite the LCD labelling on the FCU, and the FMA annunciation on the PFD, it is still possible for pilots to commence an approach in the wrong vertical mode, i.e., vertical speed rather than flight path angle. Under pressure, the tendency is merely to look at the figures one is selecting, and the figures themselves look almost identical in both modes. The selection of FPA merely adds a decimal point. I have seen a non-precision approach commenced with the selection of 3000 fpm instead of 3.0 and the result was quite exciting. The FCU figures in FPA mode should be made to look quite different - e.g. the figure after the decimal point in small font."

An important point is that automatic control of the airplane can lead to a mismanaged energy state, just as manual control can. The FBW protections in the A320 are designed to provide high-speed, loaded, and slow-speed protections. It does nothing to stop the pilot from managing the airplane in such a manner that it gets dangerously close to an obstruction (the ground) without enough energy--or even too much energy--to pull out of danger. This is what Airbus claimed happened with the crashes at Habsheim and Bangalore, with the pilots flying manually and dealing with the FCU, respectively. Airbus's Bernard Ziegler's "black holes": energy states the airplane could not recover from.

Airbus is faced with the contradictory problems of "protecting" against gross incompetence (safety issues which IT defined as problems, and which its marketing people ran away with), without being able to "protect" from the types of mismanagement their own extreme, and unrealistic, protections appear to engender. Far from changing its interface, it long ago froze it, for use in its newest aircraft, the A330 and A340, thus assuring commonality in training--and theoretically ensuring a market share among airlines who have bought heavily into the A320. But I digress. :-)

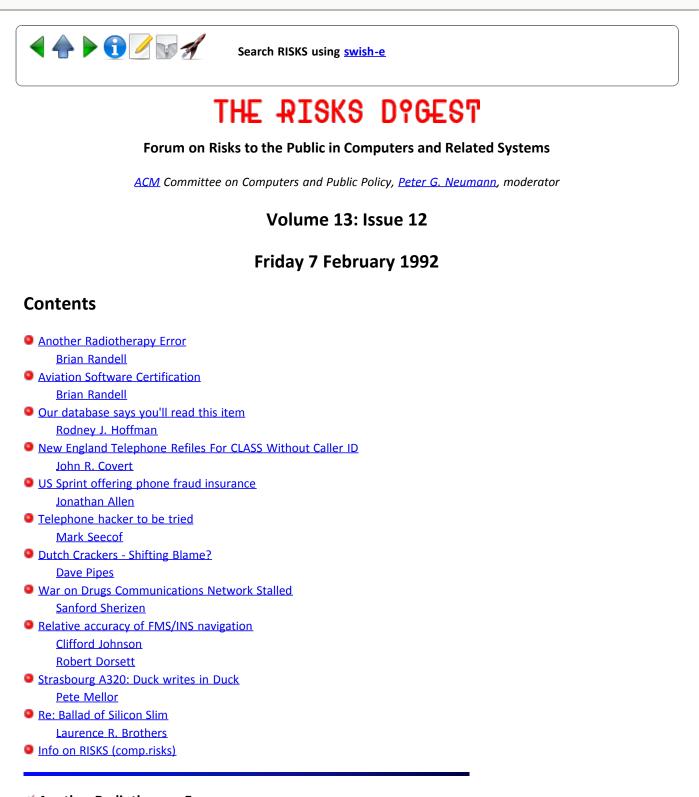
If nothing else, I hope I've made the point that FBW is NOT equivalent to flight management. FBW computers are relatively simple and straight-forward in design and purpose: FMSs are fairly complex software/hardware packages. The correct functioning of them is important (especially when used in certain ways), but not as ESSENTIAL as the FBW system.

In addition, note that the A320's automation includes many more services than just FMS-derived and FBW: there are various mechanisms to display and control systems information, warning and caution computers, etc. It's also important to note that the A320's cockpit design concept (with the exception of sidesticks and throttle management) is fairly close to that of other airplanes in production or development at this time (747-400, 777, MD-11, etc). FMS is not unique to the A320, although its actual integrated environment (as with all the airframe vendors) is proprietary and unique.

Irritating Jargon:

ATC	Air Traffic Control autothrottle A mechanism for controlling
	aircraft speed from the autopilot.
CDU	Control Data Unit
DME	Distance Measuring Equipment/station.
EICAS	Engine Indication and Crew Alerting System.
FBW	Fly by Wire.
FCU	Flight Control Unit.
fix	A geographic point, designated by the FAA as a reference point.
	Used in navigation and routing by ATC.

FMC	Flight Management Computer.	
FMGS	Flight Management and Guidance System.	
FMS	Flight Management System.	
IFR	Instrument Flight Rules.	
ICAO	International Civil Aviation Organization.	
ILS	Instrument Landing System.	
INS	Inertial Navigation System.	
IRS	Inertial Reference System.	
KAL	Korean Airlines.	
PFD	Primary Flight Display	
VOR	VHF Omni Range.	
Robert I	Dorsett rdd@cactus.org UUCP:cs.utexas.edu!cactus.org!rdd	
	Search RISKS using swish-e	
Report problems with the web pages to the maintainer		



# Another Radiotherapy Error

<Brian.Randell@newcastle.ac.uk> Fri, 7 Feb 92 10:19:55 GMT

The following article about faulty computer control of radiotherapy treatment is reprinted in its entirety, from today's Independent, a "quality" national paper here in the UK. The story was covered last night on BBC TV news - where interestingly enough they referred only to "human error", if my memory serves me correctly, and where some of the medical experts they sought comments from expressed fears that the fault might well have led to some fatalities.

Brian Randell Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, PHONE = +44 91 222 7923

#### HOSPITAL ADMITS ERROR IN TREATING CANCER PATIENTS (By John Arlidge)

Nearly 1,000 cancer patients were given radiotherapy treatment up to 30 per cent below the proper level, North Staffordshire hospital centre said yesterday. A computer programming error meant that for the last 10 years patients at the hospital in Stoke-on-Trent received doses between 10 and 30 per cent below the required level.

Stuart Gray, the hospital general manager, said yesterday: "We very much regret that an error has been made. We are very concerned about it and the staff of the department are very upset." The 447 surviving patients and their general practitioners have been informed. Patients and relatives of the 542 who have died who "need reassurance" can see consultants or call a telephone hotline set up by the hospital. Officials say there is no evidence that patients have suffered. "It is up to individuals whether they seek compensation from the district health authority," a spokesman said.

Most of the patients, from as far away as North Wales and Cheshire, were suffering from cancer of the bladder, pelvis, lung and throat. No children or patients with breast cancers or brain tumours were treated.

The physicist who made the mistake by introducing an unnecessary correction factor when a new planning computer was installed in 1982, has been transferred to another department while two doctors carry out an independent inquiry. Colleagues said she was "devastated" after realising her error when the equipment was replaced just before Christmas. Mr. Gray said it was too early to say whether there would be disciplinary action.

The Department of Health, which has been investigating the incident since December, welcomed the independent review. A spokesman said: "There is no doubt that negligence was involved. An error has been admitted... If there are any lessons to be learnt they will be implemented."

Mr. Gray said consultants have reviewed the case notes of all 989 patients treated and have found no evidence that patients had died or suffered because they received the low doses. "We have no reason to believe this has had a deleterious effect on the health of any of our patients.... We would welcome an independent inquiry to confirm the findings of our consultants."

Two senior radiotherapists - Dr. Thelma Bates of St. Thomas Hospital, London, and Dr. Daniel Ash of Cookridge Hospital, Leeds - are to carry out the independent clinical review. "We want to determine why it happened, why it went undetected for 10 years and to make sure it never happens again," Mr. Gray said.

[The Therac 25 case was one of OVERdoses being life critical. It is appropriate to note that UNDERdoses may also be life critical. PGN]

## Aviation Software Certification

<Brian.Randell@newcastle.ac.uk> Thu, 6 Feb 92 18:41:58 GMT

The front page of today's issue of the (UK) Computer Weekly is dominated by a photo of a very stern-looking Bev Littlewood, under the main headline stating "Experts warned CAA before Airbus disaster". The article is by Tony Collins.

Software experts warned the Civil Aviation Authority (CAA) that rules governing the safety of software in aircraft were inadequate two weeks before January's crash of the A320 Airbus jet in France. The results of an enquiry into the January 20 Airbus crash, which killed 87, are not yet known, but the disaster has focussed attention on aircraft such as the A320 which has fly-by-wire controls dependent on the software.

Safety-critical software experts from the British Computer Society (BCS) met the CAA to express concern about the laxity and ambiguity of certification criteria used by regulatory authorities to test the safety of complex software in aircraft. They also called for improvements in an aviation software certification codebook, D0/178B, which is now in draft form. They complained that D0/178B fails to lay down mandatory requirements for aircraft software safety and relies instead on guidelines.

The delegation to the CAA was led by Brian Wichmann, a software engineering specialist at the government's National Physical Laboratory and acting chairman of the BCS's task force on safety related systems.

Airbus Industrie, based in Toulouse, southern France said this week that it has demonstrated that the A320 and its systems fully meet the requirements of the world's certification authorities. But the delegation said that the safety claims made by the aircraft manufacturers for the software cannot be adequately tested. One member said that the committees which lay down certification standards represent the manufacturers' interests more than those of the consumer.

Another member of the delegation, Bev Littlewood, professor of software engineering at London's City University, said that some parts of DO/178B were "appalling". He said that it fails to stipulate the way in which the claims made for the software's safety by manufacturer can be tested.

The delegation's third member, Martyn Thomas, chairman of Bath software house Praxis, said aircraft manufacturers should have to prove that their software can be easily analyzed to check for any flaws. Certification standards make no provision for this, he said.

A CAA spokesman said he sympathasised with views expressed by the delegation and added that it is also seeking tougher standards for testing safety-critical software.

Clearly the paper has sought to dramatize its account of a meeting by linking it so directly to the A320. However I note that the article is followed up by

a very supportive and reasonably well-argued editorial on page 23 - an editorial which ends "The CAA is said to agree with many of the BCS objections to the DO/178B guidelines. Only with international support can it make any changes." Brian Randell

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 91 222 7923 FAX = +44 91 222 8232

### ✓ Our database says you'll read this item

Rodney J. Hoffman <rodney@oxy.edu> 04 Feb 92 12:55:21 PST

Edited bits from a story in the weekly "Marketing" column by Bruce Horovitz in the "Los Angeles Times" 4-Feb-92, p. D6:

OUR DATABASE SAYS YOU'LL READ THIS COLUMN

"If you need a stiff drink before reading this column, .... the folks at Seagram Co. already have a pretty good idea who you are. And they'll prove that in this month's issues of Newsweek, Atlantic, and U.S. News and World Report. If the marketing gurus at Seagram suspect that you're a drinker -- or are a likely candidate ... -- you'll be seeing their ads in your February issues. But if their research tells them that you're a teetotaling subscriber, don't expect to see their ads....

"Beginning this month, for the first time on a large scale, a major advertiser -- Seagram -- will test the ability of a handful of national magazines to selectively place its ads only in those issues subscribed to by likely buyers of its liquor....

"Marketers are watching more closely than ever whether consumers eat Wheaties, collect colorized movies or take frequent trips to Toledo.... How deos Seagram get this kind of personal information? Officials there declined to return phone calls. But typically, [it] is gleaned from elaborate databases on consumers who order from catalogues, telephone toll-free numbers, or even fill out questionnaires when renewing magazine subscriptions....

" 'No one wants to get involved in an invasion of privacy,' says James R. Guthrie, Exec. V.P. of marketing at Magazine Publishers of America. 'But there is no doubt in my mind that this is the direction that magazine publishing is going.' This is just the beginning. Before the end of the decade, marketing experts say, many of the advertisers in major national magazines will do individualized advertising regularly. And within 20 years, they say, most of the advertising placed in each issue of every major magazine will be targeted specifically to narrow groups of subscribers....

[Approving quotes from marketers for Lexus, Reebok, etc., and other magazines]

"But not everyone is enamored of the concept. 'We're not going to do it,' said Richard McEvoy, Senior V.P. at Carillon Importers, which imports Absolut vodka. 'It sounds like a good idea, but you won't bring in new customers if you only advertise to old ones."

# Mew England Telephone Refiles For CLASS Without Caller ID

John R. Covert 04-Feb-1992 1015 <covert@covert.enet.dec.com> Tue, 4 Feb 92 07:28:24 PST

[From: TELECOM Digest Tue, 4 Feb 92 20:30:41 CST Volume 12 : Issue 114] [from Marc Rotenberg <Marc\_Rotenberg@washofc.cpsr.org> via Lance J. Hoffman <hoffman@seas.gwu.edu>]

As a result of the Massachusetts DPU's order requiring free per-line blocking, New England Telephone has refiled for three of the original four "PhoneSmart" (CLASS) features in the original filing.

N.E.T. proposes to offer Call Trace, Return Call, and Repeat Call, but not Caller ID or any of the other features that are part of CLASS such as Incoming Call Blocking, Selective Call Forwarding. The last two were not part of the original filing.

N.E.T. had proposed a monthly fee for Call Trace as well as a charge for each use; the DPU ordered that it be provided free on all lines with only a per-use charge.

Call Trace will provide the needed protection from annoyance calls without the privacy problems.

john

## ✓ US Sprint offering phone fraud insurance

<jpallen@ics.uci.edu> Thu, 06 Feb 92 13:34:28 -0800

It's been reported that US Sprint is trying to "transform a billion-dollar industrywide problem into a source of income" by offering phone fraud insurance to its customers (Information Week, 2/3/92). Discussions about the conflict of interest inherent in making a "security industry" financially dependent on a thriving security problem suddenly seem much less far-fetched...

Is security against phone fraud something that Sprint, a company that doesn't require the use of PINs on their calling cards, should be asking its customers to pay for?

Jonathan Allen, University of California, Irvine CORPS (Computers, ORganizations, Policy, and Society) program

## Telephone hacker to be tried

Mark Seecof <marks@capnet.latimes.com>

Wed, 5 Feb 92 17:27:50 -0800

"Man To Be Tried on Phone Hacking Charges" by Jonathan Gaw. From the Los Angeles Times, Wednesday, February 5, 1992, page B8.

[Excerpted by Mark Seecof; elisions and bracketed interjections mine as well as all errors -MS.]

VISTA-A telephone hacker who allegedly tied up lines at Palomar Hospital for hours at a time has been ordered to stand trial on dozens of felony wiretapping and eavesdropping counts. Rick Ivkovich is accused of using his touch-tone telephone to jam the lines of the Escondido hospital, bringing switchboard operators to tears. From as early as April, 1990, prosecutors allege, he occasionally blocked calls to and from the hospital and connected hospital operators to outside lines, including 911 emergency lines and the county jail here. He also allegedly reported false emergencies to 911 while making it appear that he was calling from the hospital.

[Various quotes about stuff the defendant allegedly did.]

Outside the courtroom, Deputy District Attorney James Valiant [dig that name!] said lvkovich "had a gripe with the operators at Palomar. He wanted to use their telephone system and he wasn't allowed to."

[Ivkovich has been confined for treatment in Palomar Hospital's mental-health unit in the past.]

Ivkovich is charged with 18 counts of wiretapping, 18 counts of eavesdropping, and nine counts of falsely reporting an emergency, all felonies. Escondido police tracked down lvkovich in December through a series of telephone "traps."

Public Defender William Saunders argued that there may have been no violation of the law. "The calls are not private communications as required in the (eavesdropping) statute. First of all, he's a party to the call," Saunders told the court. "Any call to 911 is a taped call... and I don't think there is any expectation of privacy there." Saunders argued that wiretapping charges require physical attachment to telephone lines, and Ivkovich had none.

But Vista Municipal Judge Harley Earwicker said "there was an unauthorized connection," which met the wiretapping provisions.

[Mark Seecof <marks@latimes.com> (Los Angeles Times) says: The big question here is why Palomar Hospital couldn't (apparently) keep this guy from hacking their PBX. They should have just frozen him out. Why did the whole episode get as far as an arrest and felony charges?]

## M Dutch Crackers - Shifting Blame? (Gonggrijp, <u>RISKS-13.11</u>)

Dave Pipes x4552 <dpipes@srg.srg.af.mil> Fri, 7 Feb 92 11:11:35 EST

Rop Gonggrijp writes: [...]

"...A well trained system-manager can protect a system without making it inaccessible to normal users."

Mr. Gonggrijp's argument seems to be that the hackers could not have really broken in, as the system was reasonably well protected. Therefore, it must have been the "fault" of the system managers that they got in, because they did not do what was needed and (he implies) were not well-trained enough to do what was needed. Ergo, the hackers \*really\* got in because the system was \*not\* well-protected, and hence should bear no responsibility for any costs incurred in cleaning up after them.

Resting a plea for openness and continued ignoring of crackers on such a contradictory argument seems foolish, to say the least. By this reasoning, the two gentleman should be let go, and the system managers arrested, perhaps for recklessly endangering the data of their customers.

Why are all the pro-cracker arguments of the form of "Yes, I did it, but it is not my fault, because {blame someone else here}"? The risk? People who buy into this line of "reasoning" will feel that it is their moral obligation to chastise those who they can victimize. After all, the damage is not real, just lines on a screen 2000 miles away, and anyway the bozo had it coming...

**David Pipes** 

## War on Drugs Communications Network Stalled

Sanford Sherizen <0003965782@mcimail.com> Thu, 6 Feb 92 15:10 GMT

The New York Times reported today (6 February) that a \$617 million communications network designed to combat drugs is caught in a budget squeeze and will not be completed for at least nine years. The network, designed by the Pentagon and law enforcement agencies, was developed due to consistent communications problems in fighting drugs.

## Kelative accuracy of FMS/INS navigation (Dorsett, <u>RISKS-13.11</u>)

"Clifford Johnson" <Cliff@Forsythe.Stanford.EDU> Thu, 6 Feb 92 15:43:36 PST

In his otherwise excellent posting, in contrasting FMS with INS, Robert Dorsett states that "the potential for a KAL 007 sort of mismanagement is minimal," implying that INS-related problems were to blame for KAL 007's massive deviation. But INS-related theories are debunked in R.W. Johnson's book "Shootdown" (including the theory later relied on in Hersh's book). More importantly, the jury in the KAL 007 case found that the deviation was, as a matter of law, "intentional" and "willful." KAL was accordingly held liable, whereas the case against the manufacturers of the INS dismissed. The INS was found to be not a credible proximate cause of KAL 007's deviation.

## Kelative safety of INS/FMS]

Robert Dorsett <rdd@cactus.org> Wed, 5 Feb 92 20:08:45 CST

[Robert had this statement in response to an earlier private exchange with Cliff, but it seems appropriate to include it here. PGN]

I didn't mean to claim that there was one singular authoritative cause of KAL 007's demise. At least two books (and many net discussions, including RISKS) put forth a credible theory that a misplanted number may have thrown the track off the requisite number of miles. I should have made the nature and character of my comment more precise. [...]

Robert

### Strasbourg A320: Duck writes in Duck

### Pete Mellor <pm@cs.city.ac.uk> Thu, 6 Feb 92 17:35:37 GMT

"Le Canard Enchaine" ("The Chained Duck") is a satirical French rag which specialises in political commentary of the less respectful variety. It maintains a high standard of investigative journalism, and is not afraid to ask awkward questions. The nearest equivalents are "Private Eye" (UK) and "Der Spiegel" (Germany).

One of our French colleagues faxed us a recent article from "The Duck". By coincidence, it was written by a certain Jerome Canard (and no jokes about his brother Donald, please! :-).

As usual, RISKS readers will have to bear with my own limited ability to translate French into something that might pass for English. [Translator's, and other, notes in brackets.] :-

Disconnected alarm system on the Air Inter Airbus

The "Flight Analysis Report" [I'm not sure of the exact title of this document in English] of Air France is confidential. Pity! Its last number, dated 18 December 1991, reports five cases where the pilots, thanks to the GPWS (Ground Proximity Warning System), were able to conclude their flights successfully. This was not the case with the Lyon-Strasbourg A-320.

Explanation: This GPWS is an alarm system which is triggered by five "modes": excessive rate of descent, excessive rate of approach to the ground, loss of altitude, etc. Among the five incidents noted by the Air France document, two concern the A-320. The first was a non-stabilised "approach", the second a rapid "approach" [to the ground (?)]. Thanks to the GPWS, their pilots avoided the crash.

#### Forbidden alarm

All the aircraft of that type are equipped with this system provided by the

manufacturer. Even the A-320s of Air Inter. Alas, they had been "disarmed", as "Le Point" [a publication which I don't know] wrote. For what reason? "The company only serves the Hexagon," it was explained with a slightly bothered air [i.e., "Don't ask stupid questions!"]. "The pilots know the terrain perfectly." [Anyone know exactly which region the "Hexagon" is?]

One fact has been established: when the Lyon-Strasbourg Airbus, which was making a VOR-DME instrument "approach", was judged "clear" by the radar, it was at an altitude of 5000 feet (1600m) and 5 nautical miles (9.5km) from the start of the landing strip. In 3 [nautical] miles and one minute, it had lost 2700 feet and struck the side of Mont St. Odile.

It is there that the essential cause of the drama resides. The experts, without a doubt, will be astonished at the disconnection of the famous GPWS, all the more so since, on 12 December 1991, M. Frantzen, director of the aeronautical training and technical control service, enjoined Air Inter by letter to "reconnect" these alarm systems. Il s'est fait envoyer sur les roses. [I think this means he was told to \*\*\*\* off, but any French reader is welcome to correct me!]

## Ke: Ballad of Silicon Slim - v13 i10

Laurence R. Brothers <quasar@puddle.bellcore.com> Tue, 4 Feb 92 15:28:38 -0500

Actually, on Neil Young's old album "Trans" (lots of computer-related songs, but for some reason not released on CD), there is a song called "Computer Cowboy (aka Syscrusher)", from which I quote:

"Ride along computer cowboy, To the city just in time, To bring another system down, And leave your alias behind...

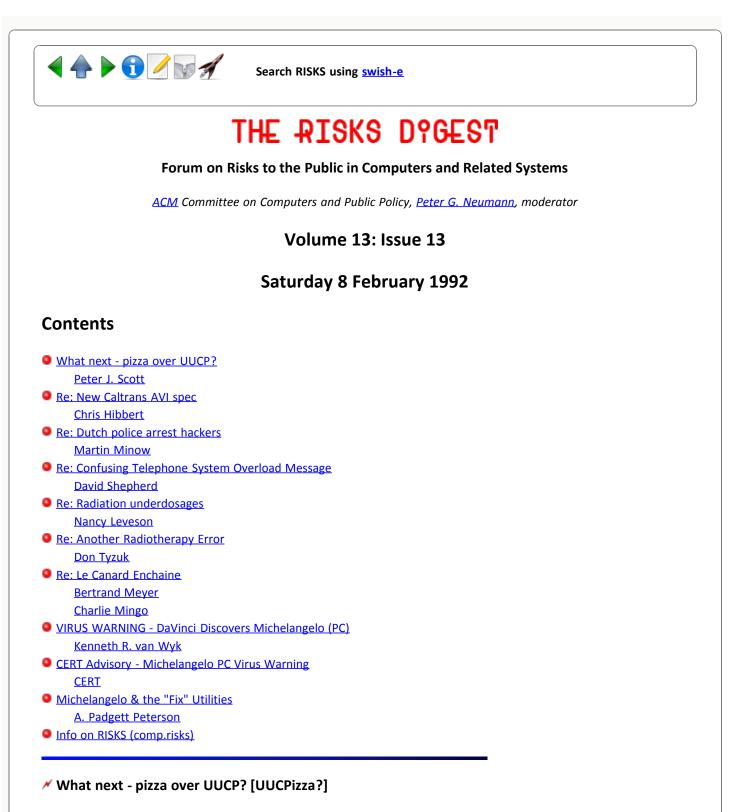
... another ballad, I imagine one of the first mass-marketed popular songs celebrating the computer intruder. I think, by the way, the song was actually released prior to the book Neuromancer, so the coincidence of "computer cowboy" is rather odd.

Laurence R. Brothers (quasar@bellcore.com)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter J. Scott <pjs@euclid.JPL.NASA.GOV> Fri, 7 Feb 92 17:15:30 -0800

A colleague just gave me this juicy tidbit. Seems that his brother-in-law was with the 82nd Airborne and, upon assignment to Fort Bragg, was given an office that had never been used. He plugged a phone into the jack and the phone immediately rang. No, it wasn't telemarketers; he was greeted with a modem tone instead. Hung up. Phone immediately rang again. This repeated 24 hours a day until the Army put a trace on the call. The trace led to, get this, a Coca-Cola machine. The manufacturer had built into these vending machines the capability to call the bottling company when they were getting low on supplies and order more.

Unfortunately for my friend's brother-in-law, the bottling company that owned this machine in particular wasn't interested in this option, so they didn't change the default telephone number that was programmed into the machine, and which was happened to be set to, you guessed it, the office at Fort Bragg.

The Army cut the telephone cable on the Coke machine. (I guess they weren't armed at the time.) This brand of vending machine also has the capability of signalling via modem that it was out of change, full up on money, or had been broken into ("Help, I've fallen over and I can't get up...").

[Not high enough on Coke? PGN]

I suppose modern machines just use FDDI. Maybe PGN could add a few candy machines to the RISKS distribution?

Peter J. Scott, Member of Technical Staff | pjs@euclid.jpl.nasa.gov Jet Propulsion Laboratory, NASA/Caltech | SPAN: GROUCH::PJS

[The RISKS archives remind us of an earlier episode with Coke machines, reported 15 Jan 1985 in the Washington Post, describing a business from which hundreds of phone calls were billed mysteriously nights and weekends even though no one was in the building. Yes, their Coke machine was trying to phone home. See ACM Software Engineering Notes, vol, 10, no 2, April 1985, p.8, four months before we started the on-line RISKS! By the way, the latest SEN RISKS index is in the January 1992 SEN issue, just out. The New Orleans SIGSOFT '91 Proceedings are in the December issue. PGN]

### Ke: New Caltrans AVI spec (Agre, <u>RISKS-13.09</u>)

<xanadu!hibbert@uunet.UU.NET> Fri, 7 Feb 92 18:21:44 PST

I also received a revision of the specification for Automatic Vehicle Identification (AVI) equipment that Phil Agre talked about in <u>Risks 13.09</u>, and that I've talked about here before. I'm much happier than Phil was with the new draft. It still has lots of problems, not the least of them the lack of attention to security. However, they've done just what I wanted on the subject of privacy.

I testified before a CalTrans hearing in October on the spec, and a state Senate Judiciary Committee hearing on Privacy in December, and it appears that my message got through. The new draft doesn't leave room for an identifier of the vehicle or the driver in the communication packets. At the hearing in December, Senator Bill Lockyer, the chair of the committee, made it clear to the head of CalTrans and to Les Kubel, who is responsible for collecting comments, that they were going to support anonymity in their system. That's a major victory.

On to the rest of the spec. First, it won't be easy to forward a copy of the

spec via EMail. The current draft is presented as a marked-up copy of the previous ones, even though it has changed massively. All deletions are presented with strike-through, insertions have double-underline, and all unchanged text has a single underline. Besides making it very difficult to read, this also means that a scanner isn't going to be able to figure it out. Oh well.

Phil misinterpreted some of the spec in his message, and asked some questions that I can answer.

From: pagre@weber.ucsd.edu (Phil Agre)

the state envisages attaching [the box] to your car that broadcasts your car's vehicle identification number (VIN) when pinged by a roadsite transmitter.

They aren't going to use VIN. The spec mentions a Reader ID number which is a 32 bit field that would identify the reader unit. This is as opposed to the first version, which said VIN, and the second that said "Character-based ID, identifying the vehicle.

would it be necessary for every car on the road to have one of these transmitters.

All the CalTrans folk and vendors I've talked to say that there's no need for every car to have one in order to collect tolls. Some are willing to say that they expect "other forces" (maybe DEA or INS?) to try to make this kind of equipment usable for tracing people's movements. There may have been attempts to make this be standard equipment on new cars. Lockyer appeared to say that the California AVI spec had better not support this "feature".

Caltrans has generalized the proposal; the "AVI" equipment is no longer specifically aimed at toll collection but is now intended to support a much wider range of applications.

I'll have to look at the old spec, to figure out why, but I always understood this to be the intent. I specifically remember that the previous version said that more packet types could be added later to serve other purposes.

I cannot understand how automatic toll collection could work unless every car has a transponder.

The spec doesn't talk about it because it's not part of the technology being designed. The following is my guess, based on how I'd build such a system. For corroboration, we should ask someone who uses the existing systems in Dallas, New Orleans, or elsewhere what their systems do. I would expect any such (toll-collection) system to be prepared for vehicles without a transponder. Some vehicles will be from out of state, some batteries will die. So, you just have cash lanes. This also allows you to take care of the cars with boxes that have run out of credit: As you approach the toll point, a sensor queries your box to find out how your balance stands. If your account is low, you see an overhead sign directing you to use the cash lane.

This doesn't make it possible to collect tolls every half-mile, but it's fully capable of supporting toll roads like the ones we currently have, or private toll roads, which could be limited to vehicles which had the units.

Phil is right, however that there are lots of other issues which are left unaddressed by the spec. The folks at CalTrans aren't interested in listening to these, so you might as well address them to your state congresscritter. There's a new draft with a new deadline of February 28, so if you want a copy or to comment on the spec itself, write to:

Les Kubel, Chief Office of Electrical and Electronics Engineering Department of New Technology, Materials and Research PO Box 19128 Sacramento, California 95819-0128

Chris

### Ke: Dutch police arrest hackers (<u>RISKS-13.11</u>)

Martin Minow <minow@ranger.enet.dec.com> Fri, 7 Feb 92 17:54:12 PST

I must strongly disagree with the following comment in the discussion of the damages caused by the Dutch hacker's break-ins:

>If restoring back-ups costs tens of thousands of guilders, something is >terribly wrong at the VU. Every system manager that uses a legal copy of the >operating system has a distribution version within easy reach.

Rebuilding the operating system for a small workstation takes at least a half-day. Re-editing all site-specific files, such as pasword files, network host tables, mail aliases, and all site-specific privileged files will certainly take several more days. For a large site with networked disks and distributed resources, the cleanup must extend to all other systems that the transgressors may have reached. This is a difficult and non-trivial task.

Please do not assume that I agree with other statements in the article.

Martin Minow minow@ranger.enet.dec.com

### Ke: Confusing Telephone System Overload Message (McCulley, <u>RISKS-13.09</u>)

David Shepherd <des@inmos.com> Fri, 7 Feb 92 10:51:30 GMT

Here in the UK the BBC had a quiz on a Saturday night show - during the show they asked a simple question and you phoned in the answer and a randomly selected person with the correct answer was phoned back at the end and told what prize a "celebrity" had won for then (the quotes are due to the fact the the first "celebrity" was Eddie the Eagle - the UK's famously bad ski-jumper). The next week British Telecom announced that during the show 1.25 million calls had been attempted on the line, but only 7,000 had been answered by the BBC!

In the past the BBC have had phone polls e.g. on capital punishment when that was being debated in parliament, and people complained that the 50-50 result was due to the capacity of the phone system and not public opinion as both lines seem to have become overloaded.

david shepherd: des@inmos.co.uk or des@inmos.com tel: 0454-616616 x 625 inmos ltd, 1000 aztec west, almondsbury, bristol, bs12 4sq

### Kadiation underdosages

<leveson@cs.washington.edu> Sat, 08 Feb 92 16:03:53 -0800

Does anyone have any other information about this than the newspaper article? The account in the Independent doesn't make it sound like it was a computer error although the article appears to blame the computer.

The following article about faulty computer control of radiotherapy treatment is reprinted in its entirety ...

A computer programming error meant that ...

But it later says that:

The physicist who made the mistake by introducing an unnecessary correction factor when a new planning computer was installed in 1982 ....

Medical physicists compute the dosage to be given to the patient (using physicians instructions about desired treatment). If the physicist did not know how to compute a proper dosage, it does not matter whether the computation was done by hand, on a calculator, or by a computer. It seems strange to blame this on a programming error. Did the physicist really do the programming? Was there treatment planning software already installed on the computer and the physicist just entered some factors (i.e., data)? If the programmer was told by an expert to implement a particular formula that is incorrect, how could this error ever be found by testing or any other method that involved software engineering techniques? If a person drives a car into a fence, is it reasonable to blame the car?

This is not at all related to what happened with the Therac-25.

nancy

### Re: Another Radiotherapy Error

Don Tyzuk <841613t@aucs.acadiau.ca> Sat, 8 Feb 1992 13:54:18 GMT With regard to computer risks in general:

I think it is time to establish licensing of software engineers, and that there should be an independant review body for such critical software of the sort that we literally place our lives directly in its care.

Many programmers of such systems have no knowledge whatsoever of the techniques of reliable programming. They were the scientist, or expert, or whatever on the object under software control, and were chosen to write the program because they could hack out something that worked.

Consequently, they turn out spaghetti. Do you want your child to be the next Therac victim?

The moniker "software engineer" is used a little loosley, for my mind. I think there is a place for real software enginners, with the education in applied science that it implies.

A program (5 years in Nova Scotia) of 2 years of applied science 3 years of software science professional experience. comprehensive examinations. membership in a professional society of engineers. a provincial license. a review committee.

No, I am not an engineer.

Donald Tyzuk Wolfville, Nova Scotia 841613t@aucs.acadiau.ca

### 🗡 Le Canard Enchaine

Bertrand Meyer @ Interactive Software Engineering Inc. <bertrand@eiffel.com> Sat, 8 Feb 92 12:55:21 PST

> By coincidence, it was written by a certain Jerome Canard (and no jokes about > his brother Donald, please! :-). <It's an old canard, anyway. PGN>

Of course not a coincidence. As every reader of Le Canard knows, ``Jerome Canard'' is a pseudonym. The choice of pseudonym indicates that articles with this signature are probably written by the editor-in-chief, or at least a quite senior editor.

> [Anyone know exactly which region the "Hexagon" is?]

Please think for half a second, or look at a map. ``The Hexagon'' means France. It's a term favored by bureaucrats and journalists. (``Today, at the four corners of the Hexagon, ...'' is a famous parody of technocratic style.)

``Le Point'' is one the four major weekly news magazines. (The others are Le Nouvel Observateur, L'Express and L'Evenement du Jeudi.)

Bertrand Meyer

[Also noted by Martin Minow <minow@ranger.enet.dec.com>]

### Ke: Strasbourg A320: Duck Writes in Duck

Charlie Mingo <Charlie.Mingo@p0.f70.n109.z1.fidonet.org> 08 Feb 92 13:01:31

[...] The term came into use in the 1960's after the loss of Algeria had blurred the French sense of where their borders lay. (Not too long ago, France included much of Africa and the Middle East, along with bits of the Caribbean, Latin America and Pacific Oceana.)

The term is the French equivalent of "the lower 48" in the US.

## VIRUS WARNING - DaVinci Discovers Michelangelo (PC) [VIRUS-L V5 #21]

"The Moderator Kenneth R. van Wyk" <krvw@CERT.SEI.CMU.EDU> Tue, 4 Feb 1992 09:40:50 EST

VIRUS-L Digest Tuesday, 4 Feb 1992 Volume 5 : Issue 21

Date: Tue, 04 Feb 92 08:22:01 -0500 From: "Kenneth R. van Wyk" <krvw@cert.sei.cmu.edu> Subject: VIRUS WARNING - DaVinci Discovers Michelangelo (PC)

[Moderator's note: I received the following press release by FAX. Any typos are no doubt mine, not DaVinci's. krvw]

News Release

DaVinci Systems Corporation, P.O. Box 17449, Raleigh, North Carolina 27619 Tel: (919) 881-4320 Fax: (919) 787-3550

Contact: Chris Evans, Vice President of Marketing, DaVinci Systems Corporation, (919) 881-4320

DaVinci Discovers Michelangelo Virus Warns users of possible infection

RALEIGH, North Carolina, February 1, 1992 - DaVinci Systems announced today that a recent shipment of eMAIL 2.0 demonstration disks and 30-day kits may be infected with a computer virus known as Michelangelo. Approximately 900 customers and potential customers were sent the infected disks. Of these, over 600 were DaVinci resellers.

DaVinci Systems immediately notified its resellers of the problem via electronic mail and will mail a new set of disks to all recipients of the infected disks by February 6th. DaVinci Systems also advises anyone who has received a DaVinci eMAIL 2.0 demo disk or 30-day kit between January 20, 1992 and January 31st, 1992 not to use the disks they received. According to Bill Nussey, President of DaVinci Systems, "While there is only a slim chance of one of our customers contracting the Michelangelo virus from these disks, we wanted to take every possible precaution."

The Michelangelo virus sits passively on infected machines until March 6th (Michelangelo's Birthday) when it corrupts data on a user's hard disk. FORTUNATELY, THE VIRUS CAN ONLY BE CONTRACTED BY BOOTING UP AN INFECTED FLOPPY. Because the infected disks are not bootable, most users who have received these diskettes will not contract the virus on their machine even if they run the demo or install the software on their hard disks. The only way users could catch the virus from an infected disk is if they inadvertently boot up their computers with the infected floppy in driver A while the drive door is closed.

DaVinci officials are still investigating the source of the virus. Although DaVinci's master disks are routinely checked for viruses, the virus software used apparently did not detect Michelangelo. "We are now using multiple virus-detection products and insisting that our duplicating contractors also check for viruses", said Nussey.

The Michelangelo virus can be detected by Microcom's Virex version 2.11 or later or by McAfee Associates shareware program VIRUSCAN version 7.9v84 or later. DaVinci users and resellers can download VIRUSCAN from DaVinci's BBS at (919) 881-4342.

Based in Raleigh, North Carolina, DaVinci Systems Corporation is the leading independent supplier of LAN-based electronic mail applications. The company's products run under acknowledged personal computer network and operating system standards such as MS-DOS, Microsoft Windows, and Novell Netware. DaVinci Systems is at P.O. Box 17449, Raleigh NC 27619. Telephone (919) 881-4320, (800) DAVINCI. FAX: (919) 787-3550.

The product names and trademarks referenced are the trademarks or registered trademarks of their respective companies.

## ✓ CERT Advisory - Michelangelo PC Virus Warning

CERT Advisory <cert-advisory-request@cert.sei.cmu.edu> Thu, 6 Feb 92 15:57:37 EST

CA-92:02 CERT Advisory February 6, 1992 Michelangelo PC Virus Warning

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a personal computer virus known as Michelangelo. The virus affects IBM PCs and compatibles. A description of the virus, along with suggested countermeasures, is presented below.

I. Description

The Michelangelo virus is a computer virus that affects PCs

running MS-DOS (and PC-DOS, DR-DOS, etc.) versions 2.xx and higher. Note, however, that although the virus can only execute on PCs running these versions of DOS, it can infect and damage PC hard disks containing other PC operating systems including UNIX, OS/2, and Novell. Thus, booting an infected DOS floppy disk on a PC that has, for example, UNIX on the hard disk would infect the hard disk and would probably prevent the UNIX disk from booting. The virus infects floppy disk boot sectors and hard disk master boot records (MBRs). When the user boots from an infected floppy disk, the virus installs itself in memory and infects the partition table of the first hard disk (if found). Once the virus is installed, it will infect any floppy disk that the user accesses.

Some possible, though not conclusive, symptoms of the Michelangelo virus include a reduction in free/total memory by 2048 bytes, and some floppy disks that become unusable or display "odd" graphic characters during "DIR" commands. Additionally, integrity management products should report that the MBR has been altered.

Note that the Michelangelo virus does not display any messages on the PC screen at any time.

#### II. Impact

The Michelangelo virus triggers on any March 6. On that date, the virus overwrites critical system data, including boot and file allocation table (FAT) records, on the boot disk (floppy or hard), rendering the disk unusable. Recovering user data from a disk damaged by the Michelangelo virus will be very difficult.

#### III. Solution

Many versions of anti-virus software released after approximately October 1991 will detect and/or remove the Michelangelo virus. This includes numerous commercial, shareware, and freeware software packages. Since this virus was first detected around the middle of 1991 (after March 6, 1991), it is crucial to use current versions of these products, particularly those products that search systems for known viruses.

The CERT/CC has not formally reviewed, evaluated, or endorsed any of the anti-virus products. While some older anti-virus products may detect this virus, the CERT/CC strongly suggests that sites verify with their anti-virus product vendors that their product will detect and eradicate the Michelangelo virus.

The CERT/CC advises that all sites test for the presence of this virus before March 6, which is the trigger date. If an infection is discovered, it is essential that the user examine all floppy disks that may have come in contact with an infected machine.

As always, the CERT/CC strongly urges all sites to maintain good

backup procedures.

The CERT/CC wishes to thank for their assistance: Mr. Christoph Fischer of the Micro-BIT Virus Center (Germany), Dr. Klaus Brunnstein of the Virus Test Center (Germany), Mr. A. Padgett Peterson, P.E., of the Technical Computing Center at Martin-Marietta Corp., and Mr. Steve R. White of IBM's Thomas J. Watson Research Center.

If you believe that your system has been compromised, contact CERT/CC or your representative in FIRST (Forum of Incident Response and Security Teams).

Internet E-mail: cert@cert.sei.cmu.edu

Telephone: 412-268-7090 (24-hour hotline)

CERT/CC personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4), on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous ftp from cert.sei.cmu.edu (192.88.209.5).

## Michelangelo & the "Fix" Utilities - free through March 6th

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com> Fri, 7 Feb 92 09:37:29 -0500

This virus has really surprised me. When I first say it, my thought was "yet another STONED" (and not as well written), but it seems to be spreading & spreading... If Rob Slade's estimate is right, for every report we see, there are at least three other infected computers that we don't. March 6th may just be interesting.

Some time ago I did a number of experiments concerning boot sectors in general since we seemed to have good protection from DOS viruses but few people were working at the BIOS level before DOS ever starts. IMHO, since over 50% of the reported infections begin at the BIOS level, then that is where the checking should start. The first experiments (written in 1988) were a set of integrity checking programs, two of which were CHKMEM and CHKBOOT (now FREEWARE) that could be used to detect all "common" viruses - I presented a paper on this at last year's Virus & Security Conference in New York (March 12 & 13 this year call (800)835- 2246 x190 for info - plug).

These operate from the DOS level. About two years ago, I began studying a BIOS level approach - at this point the Intel PC is a fully functioning computer with access to all peripherals, it is just not yet a DOS (or Unix or OS/2 or...) computer.

The first result was the DISKSECURE program that was designed as a technology demonstrator & performed BIOS level integrity checking and protection of the MBR, hidden sectors, and DOS boot record. Many researchers

seem to like it as an additional layer of protection.

DISKSECURE's biggest limitation was that it could do nothing about a floppy boot (only hardware can prevent this) and I was and am convinced that a global solution had to be software based - not for technical reasons but for logistical and economic ones.

The next effort was SafeMBR - a BIOS level Master Boot Record replacement that performed integrity checking on the system and which would halt a boot if "something" was wrong and used lessons learned in DISKSECURE to avoid conflicts with the incredible array of disk controllers, BIOSes, and DOS variants that exist. SafeMBR is FREEWARE.

Late in 1991, I extended the SafeMBR concepts to a similar floppy disk replacement SafeFBR to provide a generic floppy disk boot record replacement with warning messages.

Concurrently with SafeMBR, I addressed the "floppy boot" problem as far as possible with software, a TSR (512 bytes needed & can be loaded "high") was written to intercept the Ctrl-Alt-Del sequence and test for a floppy in drive A. If one is found, the reboot is denied. This taught me more about the inner workings of the BIOS and the Interrupt Controller. NoFBoot was the result and is also FREEWARE.

The final parts FixMBR and FixFBR were extensions of this concept used to install SafeFBR and SafeMBR. FixMBR came from hours spent disinfecting machines infected by MBR viruses and was designed to automate the repair based on the fact that ALL leave an intact partition table SOMEWHERE. Given an intact partition table, all that is usually necessary is to replace the MBR program. Generally I use the SafeMBR code to do this.

For some time, I was hesitant to release these techniques but then along came the Azusa virus...

FixFBR works essentially the same way except that only four Boot Parameter Blocks are needed (does not work with 2.88 Mb floppies yet). Since it also incorporates the CHKBOOT techniques, it will also flag potentially infected disks.

This last is the key to the concept. None of these programs (well maybe NoFBoot) will prevent a virus infection. What they will do is to detect viruses almost immediately. Flag the "anomaly" in a way the user cannot ignore, and provide a recovery mechanism. They do not "identify 1000 viruses" but will tell you that "something" has happened at the BIOS level without going resident. They are designed as one layer in a layered protection (I use four layers myself).

Similarly, either CHKBOOT or FixFBR will detect the Michelangelo virus on floppy disks and report them as "suspect". FixFBR will then remove the problem.

To me this is a vital element in fighting malicious software, knowing early on that "something" has happened and isolating the abnormality to as narrow range. I personally believe that if these techniques were used globally, those viruses responsible for over half of reported infections: Stoned, Azusa, Aircop, Brain, Joshi, & Michelangelo would quickly disappear.

But today there appears to be a very real threat: Michelangelo that needs to be addressed. I have never seen so many reports of a virus in so short a time before and am particularly disturbed about the number of "shrink-wrapped" reports. Consequentially, while normally I "suggest" a nominal SHAREWARE fee (\$1.00) for the two "FIX" utilities, from now until 7 March, 1992, payment requirements are suspended and they may be freely used, posted, & transmitted without limitation so long as they are not modified.

Padgett padgett%tccslr.dnet@mmc.com

PS: I know that the current version of these programs is in FIXUTIL2.ZIP and may be found in directory msdos.antivirus at urvax.urich.edu (141.166.1.6 - thanks Claude).

Note: this is my hobby, my employer has nothing to do with this.

Programs in FIXUTIL2.ZIP

Length CRC-32 Name ----- ----1331 449b4371 CHKMEM.COM 2189 2753290a FIXFBR.EXE 368 72b99d29 SUMFBOOT.COM 1357 77936de4 CHKBOOT.EXE

2219 332bf466 FIXMBR.EXE

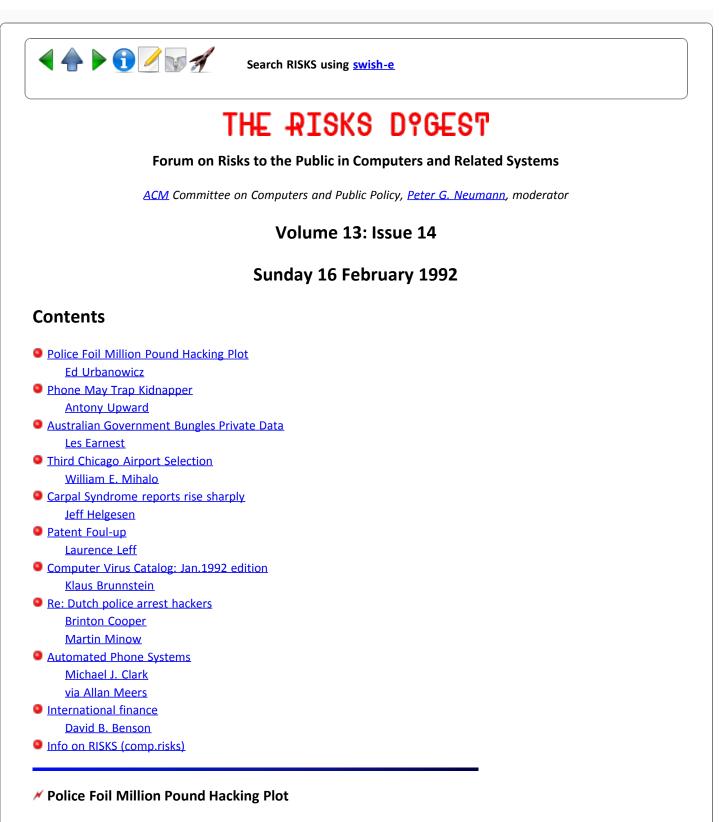
4885 3e04a29b FIXFBR1A.DOC 749 3f347828 CHKSMBR.EXE 368 cccf71a5 NOFBOOT.COM 2602 63f3d358 NOFBOOT.DOC 4461 a1408395 CHK.DOC 366 4c0e9c20 VALIDATE.24 26118 8138037e FIXMBR24.DOC

47013 12 files



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Sun, 16 Feb 92 14:47:09 PST

Ted Urbanowicz of Stow, Ohio, sent in an item from the 30 Jan 1992 issue of Computing (UK). I have abstracted.

Police have charged a woman under the Computer Misuse Act following a million pound hacking incident at a leading city finance company. Elaine Borg, a

computer operator at fund managers Henderson Financial Investment Services, is accused of hacking into the company's computer system between 1 Oct 1991 and 19 Jan 1992 with intent to defraud it of a million pounds. Borg was charged in London's City Magistrates' Court under Section Two of the Act, which covers unauthorised access to systems with the aim of assisting a more serious crime, such as fraud or blackmail. Her activities were being monitored for several days before she was apprehended. Oddly, the managing director of Henderson was quoted as saying that it would have been difficult to complete the fraud, because it would have required collusion at the other end. But the article noted that Borg faces a second charge of conspiracy with another person, Richard Hollands, while another man, Keith Cheeseman, was also arrested in connection with the fraud, but not charged because of extradition problems. Cheeseman is wanted by the FBI in connection with a multimillion pound bond theft in London two years ago.

The COMPUTING article closed with a note on a recent National Computing Centre report (Security Breaches Survey, NCC, Oxford Road, Manchester M1 7ED UK; contact David Lindsay, phone 44 6355524040), which estimates that security breaches cost UK industry 1.1 billion pounds a year.

#### 🗡 Australian Government Bungles Private Data

Les Earnest <les@sail.stanford.edu> Fri, 7 Feb 92 15:14:51 -0800

[Reposted with permission from the ClariNet Electronic Newspaper newsgroup. For more info on ClariNet, write to info@clarinet.com or phone 1-800-USE-NETS.]

SYDNEY, AUSTRALIA, 1992 FEB 6 (NB) -- Australian government officials are ducking for cover as yet another case of personal data misuse "hits the fan." More than 6,000 households received official letters containing personal and financial details about others.

Recipients of what should have been a routine Department of Social Services letter about child allowances were shocked to see a list of information about others, sometimes neighbors. The data included name, address, bank account details, tax file number, and income.

One recipient said: "I was looking at the back of the letter, assuming the information I saw was meant as an example, when a neighbor rang to say she was reading all about me on the letter she had just received. I felt sick, knowing that my private affairs had been revealed like that. They say 'give us your details - you can trust us' but we can't, can we?"

Officials from the department have given two explanations so far, though it may be some time before the complete story surfaces. The letters had correct data on the front, but incorrect data on the reverse. The first explanation was that the laser print run had faltered, and when it was restarted, the letters were printing front and back, one step out of sync. The second (and expected) excuse was that there was a glitch in the computer program which had been imported. Unfortunately for the Australian government, this was not the first incident of its type, and a large public storm is rising over the rapid increase in the amount of data held in a central computer in Australia's capital, Canberra.

### Main Chicago Airport Selection

"William E. Mihalo" <calumet!wem@apple.com> Sat, 08 Feb 1992 09:28:21 cst

The selection process for the third Chicago airport continues to generate controversy (see a previous issue of Risks Digest). In this particular case, its an excellent example of PC-based computerized mapping programs and spreadsheets being abused.

A revised configuration for the Lake Calumet site (which is strongly favored by Mayor Daley), has modified the footprint for the airport. The Ford assembly plant in Hegewisch, Illinois is now spared (this plant is used for the assembly of the Ford Taurus and Mercury Sable). However the revised footprint for the airport has it crossing the stateline into Northwest Indiana. One of the runways ends within less than a mile of the Amoco Oil Refinery in Whiting. An estimated 25,000 homes, half a dozen schools and 15 churches would need to be razed to make room for the airport. The revised plan doesn't anticipate the relocation of any industrial sites.

However it also calls for the draining of several hundred acres of wetlands. The fate of several lakes that are adjacent to the airport site is also in question. An estimated 50,000 people would be dislocated by the project.

The second risk is one of computer spreadsheets. The original cost of the airport was \$5 billion. A revised cost from Mayor Daley is \$10.8 billion. However this assumes the razing of only 10,000 homes. An estimated \$18 to 30 billion would be needed to raze the 25,000 homes that are within a 7 mile radius of the proposed site. Assuming a \$10.8 billion dollar cost a ticket surtax of \$12-15 per ticket would be levied for any flight originating or terminating from Midway and O'Hare. With the \$30 billion estimate the ticket tax would be in the range of \$36 - \$50.

The entire justification for the third airport is based on FAA data from the late 1970's which was gathered just before the deregulation of the airline industry in the United States.

One question for the Risks community. Has anyone ever estimated the area of destruction that would result if a jumbo jet was to make a direct hit upon an oil refinery? Whenever the issue of safety is mentioned it is dismissed with the statement that commercial aviation is safer than driving. O'Hare was the site of a DC-10 crash in 1979 which killed several hundred people. Indiana within the past 4 years has had two crashes (one in Indianapolis, and a more recent one in Evansville) with planes going down near airports with a significant loss of life from people on the ground.

William E. Mihalo wem@calumet.uucp

## ✓ Carpal Syndrome reports rise sharply

Jeff Helgesen <jmh@morgana.pubserv.com> Thu, 13 Feb 92 14:43:47 -0600

[The following article appeared in the Chicago Tribune, 11 Feb 1990. All typos are mine; bracketed inserts are those of the original editor.]

CARPAL SYNDROME REPORTS RISE SHARPLY (Jon Van, Chicago Tribune)

Reports of repetitive-motion disorders have risen sixfold in recent years and now account for more than half of all occupational illnesses in the United States, a report in Wednesday's Journal of the American Medical Association noted.

Physicians must work with employers, industrial designers, labor representatives and others to modify work sites so that these injuries, sometimes known as cumulative trauma disorders and sometimes as carpal tunnel syndrome, can be avoided, the report said.

The U.S. Bureau of Labor Statistics found that there were 24 cases of cumulative trauma disorder for every 10,000 U.S. workers in 1990, up from 4 cases per 10,000 in 1982.

Dr. David M. Rempel, director of the ergonomics laboratory at the University of California at San Francisco, said in his Journal report that several factors account for the increase. They include increased awareness of the problem, advances in medical diagnosis and an ever-accelerating pace of work. Even though the problem is growing, most physicians are ill-prepared to deal with it, Rempel and his colleagues said. ``Because of the scarcity of medical research on [the disorders]," they wrote, ``many physicians are unable to identify patients working in high-risk environments and are inadequately prepared to treat patients with symptomatic disorders."

When someone applies force over and over to the same group of muscles, the same joint or the tendon, the result may be tissue tears and trauma. Other factors causing damage are awkward joint posture and prolonged constrained posture.

Workers should be encouraged to watch for symptoms, especially pain, and seek medical attention early, Rempel and the co-authors said. They shouldn't be told to work through pain, the report said. ``Medical intervention for the patient with [a disorder] requires not only accurate diagnosis and appropriate therapy, but also direct involvement in changing the patient's work environment," the report concluded.

## 🗡 Patent Foul-up

Dr. Laurence Leff <mflll@uxa.ecn.bgu.edu> Sun, 9 Feb 1992 22:49:17 GMT

This RISKS submissions concerns a computer problem with a patent application.

When the patent examiner issues a final rejection of a patent, the patent office can give you a shortened time to respond. This response is an appeal to the board of patent appeals.

The statutory time to respond is six months; however the patent office has the authority to shorten this time.

You can extend the time given by the patent office by paying a late fee--however, late fees won't extend your total time more than the six months specified in the statute.

On 08/13/91, the patent examiner issued me a final rejection of my patent. The problem concerns the date on the letter informing me of this.

That letter was issued on a standardized form, PTOL-326.

That form included the statement:

"A shortened statutory period for response to this action is set to expire 3(three) month(s) 0 days from the DATE OF THIS LETTER." (Emphasis mine). The 3 for three months and the zero for 0 days were entered in handwriting.

The date was supposed to be printed on the preprinted form under or next to the preprinted text that said "Date mailed"

Unfortunately, the dot matrix printout of the date was obscured by the preprinted "Date mailed." The date printed on the letter of "08/??/91" was eighty percent obscured.

It was obvious that the form was not correctly aligned in the printer. The name of the examiner was not under the heading "examiner." And the number 231 wa not under "art unit." Thus, I couldn't read it properly and read the date as 09/10/91. The slash overlapped one of the letters which appeared to be a nine. Section 1.134 of 37 of the Code of Federal Regulations states in pertinent part,

"An office action will notify the applicant of any non-statutory or shortened statutory time period set for response to an Office action."

The office action failed to notify me of the indicated time. Thus, "unless the applicant is notified in writing that response is required in less than six months, a maximum period of six months is allowed." (37CFR 1.134). Thus, I am arguing my response was not due for six months from the indicated date as the Patent office did not fulfill it's regulatory requirement of notifying me as specified by this section.

Therefore, I requested that no fee be assessed at all.

This points out the obvious risks of not aligning forms when put into printers.

However, this likely human error was compounded by:

- 1) using a cheap nine-pin dot matrix printer with this form. If the numbers were printed with a daisy wheel printer or 24-pin printer, they would have been more readable even if printed on top of other information.
- 2) Using a numerical date format "08/13/91" instead of August 13, 91.One is less likely to confuse August and September than 08 and 09.Although "November" and "December" have most of their letters in common.
- 3) However, the patent office had the correct date in a computer system. They should have printed everything out using a laser printer including the shortened statutory time, the date of final reject and the date the response was due. All the information on the preprinted form would be printed out at the same time.

This would be a simple WordPerfect merge application.

### Computer Virus Catalog: Jan.1992 edition

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 14 Feb 92 16:54 +0100

At the end of our winter semester, the following new entries of Computer Virus Catalog are available:

INDEX.192: survey of all entries published so far (214 viruses/trojans)
AMIGAVIR.192: 14 new viruses (total: 29 viruses/time bombs)
MACVIR.192: 9 new viruses (all known 29 viruses/clones classified)
MSDOSVIR.192: 15 new viruses (total: 99 viruses, 4 trojans)
including: Amilia (Murphy Strain), AntiCAD (Jerusalem/ AntiCAD strain), FEXE & FICHV2.0 & FICHV2.1 (all: FICHV strain), Hafenstrasse (no strain), Michelangelo (Stoned strain), PLOVDIV 1.3 (PLOVDIV strain), SEMTEX, Sverdlov=Hymn of USSR, Violetta, ZeroHunt-411, -415 = Minnow/1 (ZeroHunt strain), VDV-853 (maybe VCS 1.0 predecessor).

Moreover, the first polymorphic virus using Dark Avenger "Mutating Engine 0.9" is classified, named "Dedicated".

After analysis of an accident with a UNIX shellscript virus in a European university, based on several publications of an AT&T author who described all details of the virus' code and sufficient details of his "attacks" on several UNIX systems in his enterprise, we have classified this virus under the provisional name "AT&T ATTACK virus". This information is available from the author, on specific demand; despite the fact that this classification does not contain any information helpful in programming this virus, we wish to avoid as far as possible a similar virus wave as we observer so regretfully in the PC world. This is the reason for some restrictions in distribution of the Catalog entry.

All information including all other Virus Catalog entries may be received

either by demand from the author or may be downloaded from our FTP site:

address: ftp.informatik.uni-hamburg.de 134.100.4.42 login anonymous password your-email-adress directory: pub/virus/texts/catalog

Moreover, those interested in Chaos Congress material (e.g. CCC91): these are available on the same ftp site with the same procedures in directory: pub/virus/texts/hackers

Finally, we are updating the Index of Malicious MsDos Code; to avoid those inaccuracies which unfortunately were built-into the first edition (IMSDOS.791) due to misleading information from several alternate sources, Vesselin Bontchev and I decided that we \*only publish information on those viruses/trojans etc which are in our Secure Malware Database\*. In the next edition, it will describe about 1,150 viruses/trojans with those names/aliases which are used by major antivirus software. This edition will be available on the ftp-site early in March.

All comments and critical remarks which helps us in enhancing the quality of our work and information is strongly welcomed.

Klaus Brunnstein, Virus Test Center, University of Hamburg, Germany

# Ke: Dutch police arrest hackers (Minow, <u>RISKS-13.13</u>)

Brinton Cooper <abc@BRL.MIL> Tue, 11 Feb 92 9:20:16 EST

In discusing system restoration following illegal hacker activity, Martin Minnow takes issue with the assertion, "...Every system manager that uses a legal copy of the operating system has a distribution version within easy reach." He says, in part, "Rebuilding the operating system for a small workstation takes at least a half-day. Re-editing all site-specific files, such as pasword files, network host tables, aliases..."

It seems to be RISK-y behavior not to keep an image of your operating system, including the site-specific files, on tape back-up...off-line, not available via automatic de-archiving, mountable only manually, etc. What happens when disks are corrupted by more benign influences such as power surges or head crashes?

\_Brint

[Also commented on by David Rose, dave@phoenix.pub.uu.oz.au. PGN]

# re: Brinton Cooper's comments on system recovery

Martin Minow <minow@ranger.enet.dec.com>

#### Tue, 11 Feb 92 15:47:12 PST

Brinton Cooper notes that it is "RISK-y behavior" not to keep a fullyconfigured system image on tape backup, especially in order to recover from hardware errors. He is absolutely correct. However, if your system was intentionally attacked, this might be insufficient. I know of one case where the system manager not only rebuilt the system from distribution tapes, but he even went so far as to order new tapes from the manufacturer in order to avoid the minuscule risk that the attacker had physical access to the on-site tape library. Of course, only the system owner can evaluate the tradeoff between acceptable risk and the cost of protecting against that risk. Martin Minow

#### Automated Phone Systems

Allan Meers - Sun Education/Professional Services <Allan.Meers@ebay.sun.com> Tue, 11 Feb 92 13:37:11 PST

>From rec.humor, a commentary on those over-optioned automated phone answering/messaging systems.

## AUTOMATION IN THE 20th CENTURY By Michael J. Clark

The setting is a typical bedroom, a woman is in the bed asleep, next to her bed is a night stand with an alarm clock and a telephone. Suddenly the woman awakens to the sound of a strange noise in the house, she looks around, starts to panic and then picks up her phone to call the police.

Woman: (Startled and panicked, talking out loud to herself in a low tone) "I-I-I-I've got to call the police, there's someone here, oh God I know there is, let's see...what's the number, (she nervously punches the numbers into the phone.)

After a few rings the phone is answered, there is a delay, then we hear: "Welcome to our emergency phone mate 911, the automated emergency answering system, the latest in emergency response technology! If you are calling from a touch tone phone, please enter a 1 at the tone, enter now"......(the woman looks both shocked and puzzled as she nervously punches in a "1") "Thank you, our emergency phone mate 911 recognizes that you are calling from a touch tone phone......To serve you better your police and emergency services have set up this system to route your call to the appropriate emergency service personnel.....If you are in need of police assistance enter a 5, if you require information in Spanish, enter 7, in Chinese enter 4, in Greek enter 9, in French enter 6 or Italian enter an 8, if you wish fire or medical service enter a 3 and the corresponding numerical code for the language in which you will be speaking or in need of translation.....to repeat the previous information please enter 0......Enter your code now please"......(the woman, who has now gone from fear and panic to being irritated and confused enters a 5 and waits.....) "Emergency phone mate 911 recognizes that you have requested police assistance in English....In order to better serve you, please enter the appropriate number at the tone....a 1 if your call is not an emergency, a 2 if

you need information, a 3 if you are returning a call from a police official, a 4 if you are inquiring about a parking ticket, or a 5 if this is an emergency, enter your code now".......(she shakes her head and rolls her eyes and enters a 5 quite forcefully) "Emergency phone mate 911 recognizes that you have a police emergency, please enter a 1 if it is a life threatening emergency, a 2 if it is a non life threatening emergency, a 3 if there are weapons involved, a 4 if there are multiple perpetrators, a 5 if the perpetrators are non English speaking and will require a Miranda warning in any other language....Please be sure to enter the appropriate language code if you enter a 5....if the police emergency is a non life threatening rape or physical assault please enter a 7......

(the woman now has lost her temper, she punches in a 2 saying out loud "How the hell do I know if it's life threatening or not you imbecile!) "Emergency phone mate 911 recognizes that you have a police emergency that is non life threatening, emergency phone mate will now direct your call to the appropriate department for response.....please hold while your call is transferred.....(we hear ringing......, the phone is answered) "Dunkin' Donuts, may I help you?"

### International finance

David B. Benson <dbenson@yoda.eecs.wsu.edu> Wed, 12 Feb 92 14:09:10 -0800

From: dbenson@yoda.eecs.wsu.edu (David B. Benson) To: djb@vax.ox.ac.uk (Dave Benson) Subject: Bank statement

Dear Dave,

Forwarded to me from Yale is a bank statement from Den Danske Bank originally addressed to

MATHEMATIKER, DAVID BENSON, DEPT. OF MATHEMATICS, YALE UNIVERSITY, BOX 2155, YALE ST., NEW HAVEN, CONN.06520 USA

I suspect this is yours. However, I did open it (apologies, but there was no other way to determine the original addressee) and it appears that the account is inactive.

Would you like me to send this to you anyway? (Alternatively, with your authorization, I could send you the account number and the balance via this not very secure medium of email.)

Sincerely, David B. Benson

- - - -

Date: Tue, 11 Feb 92 9:04 GMT From: DAVE BENSON <DJB@vax.oxford.ac.uk> To: DBENSON <@nsfnet-relay.ac.uk:DBENSON@YODA.EECS.WSU.edu> Subject: Bank statement

## Dear David,

I seem to be plagued in life by encountering other David Bensons. There's one living just a few miles from here who shares also my middle name and exact date of birth. I have no desire to meet this doppelg"anger in case he turns out to look just like me. As far as the bank account is concerned, I tried several times in 1982 to close it, and in the end decided just to ignore it. So please do what you like with the statement of balance of zero Kroner og zero Ore.

Zoodle wurgle, Dave Benson.

- - - -

From: dbenson@yoda.eecs.wsu.edu (David B. Benson) To: DAVE BENSON <DJB@vax.oxford.ac.uk> Subject: Re: Bank statement

I know the feeling all too well. So far, though, none with the same middle initial nor looking like me. I'll not send along the bank statement, but I fear that now Yale will, every year, forward the statement to me -- for the rest of my life.

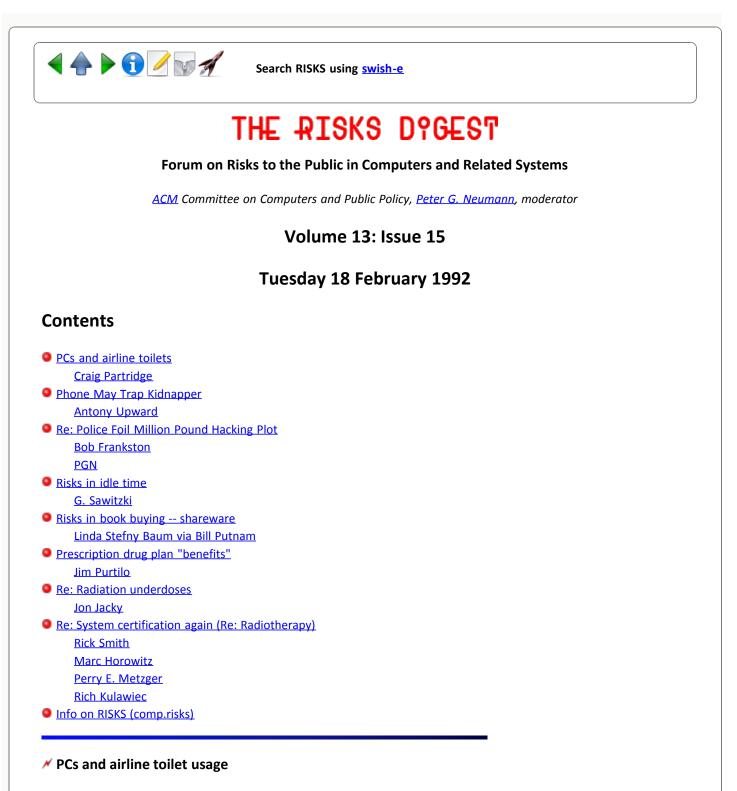
Cheers, David

[Reproduced with permission of Both Dave Bensons. But what if they start charging interest? PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Craig Partridge <craig@aland.bbn.com> Tue, 18 Feb 92 10:22:38 -0800

Apparently airline passengers with portable PCs are using the shaver outlets in the toilets to recharge their PC batteries. Since recharging a battery can take some time, this behavior dramatically reduces passenger access to toilets. [Computers constrain key bodily functions... :-)]

I've encountered three pieces of information that suggest this is not just a nice urban myth. First, two colleagues have reported encountering the problem. One on a flight to Japan (where apparently at one point, almost all the toilets were taken by folks sitting inside recharging their PC batteries), one on a flight cross the US. Second, there was an article several weeks ago (I think in the SF Chronicle travel section) on business travel that mentioned that some business travelers were now requesting seats at the back of the plane for easier access to the shaver outlets (the article suggested said passengers were using extension cords...)

### Craig Partridge

[HIT or MYTH? Not aMYTH. I noticed on last week's cross-country trip that ALL of the shaver outlets had been blocked off, with a sticker over the jack saying that this blockage was effective as of something like November 1991. A myth is as good as a mile-per-hour increase in speed. Some planes provide phone hookups in each row group; perhaps we will soon see per-seat electrical outlets as first- and business-class perks. Opportunity for a SURCHARGE? <Quadruple pun intended.> Call your favorite airline now. PGN]

## Phone May Trap Kidnapper [Missing from <u>RISKS-13.14</u>]

KPMG - Antony Upward,IVC <UPWARD.A@applelink.apple.com> 12 Feb 92 08:44 GMT

Phone May Trap Kidnapper, by Paul Cheston (London Evening Standard, 7 Feb 1992)

Detectives hunting the kidnapper of estate agent Stephanie Slater believe they can trap him through the mobile phone he used to pass on instructions for the 175,000 (pounds) ransom drop.

Courier Kevin Watts is convinced the kidnapper used a mobile phone to direct him in thick fog towards the disused railway bridge where he left the money. Mr. Watts had been ordered by the kidnapper, descirbed by police as Britain's most wanted man, to a remote phone box near Penistone outside Barnsley. Parking nearby, he carried the ransom money into the booth when the phone rang almost immediately. The ring was so fast the estate agent branch manager realised the kidnapper had been watching him and must have been using a mobile phone.

A mobile phone's unique electronic serial number is recorded by the computer which runs the network and can be used to trace the phone user.

### Ke: Police Foil Million Pound Hacking Plot

<Bob\_Frankston@frankston.std.com> Mon 17 Feb 1992 09:06 -0500

The note about extradition problems is interesting. They become especially acute with computer crimes (ecrimes?). In the old days one would commit a crime and then escape to a "safe" country. Today one can first escape and then commit the crime.

What are the implications and remedies?

## Ke: Police Foil Million Pound Hacking Plot (Frankston, <u>RISKS-13.15</u>)

"Peter G. Neumann" <neumann@csl.sri.com> Tues, 18 Feb 92 12:55:44 PST

In partial answer to Bob Frankston's question, the implications are of course quite profound. We need more international cooperation to establish and hinder what is illegal. (Cf. the US-Dutch noncommunication noted in <u>RISKS-13.11</u>, 12, 13, 14.) Might we see pirate ships from which cracking would be legal? And a new breed of international terrorism protected by safe havens? The existing international legal situation is certainly inadequate today, but it is also intrinsically limited in what it might eventually be able to do even with greater international cooperation. In addition, we need more-secure computer-communication systems, better user and system authentication, meaningful audit trails, etc., to hinder misuse. Without them, crying over electronically spilled milk money leads to ECrim(e)osus/lacrimosus/lactimosus/ galactimosus. The -osus with the mos'us is the crime that won't rhyme.

### 🗡 Risks in idle time

<gs@statlab.uni-heidelberg.de> Mon, 17 Feb 1992 14:59:04 -0800

On Jan. 27th, D.C. Lawrence reported on D. Gerlernter's "Linda" for distributed computing, and the possible lack of risk awareness shown in related trends. He asked for related trends.

In the "NetWork Project", the StatLab Heidelberg has been working on another system for distributed computing making use of idle times of workstations on a net. We agree on the critical asked by D.C. Lawrence. Here is how they are delt with in the NetWork Project.

(1) Privacy and user control. The owner should always be in full control of the machine. NetWork uses a demon as a communication agent. All communication for the NetWork system is funneled through this demon, the "NetWork Processor". This "NetWork Processor" is under full control of the owner of a machine. The owner can set up the machine not to participate in NetWork distributed computing at all. Or the owner can set up a certain threshold of idle time after which the machine can be used for distributed computing. The "NetWork Processor" takes care to repect these settings. A machine will only visible to the NetWork System if it is published and is idle in terms of the definition of the l o c a l user. And if the local user comes back, the "NetWork Processor" guaranties to remove (kill, if necessary) any guest processes immediately.

(2) Code and information security. How do you prevent the introduction of worms, and how do you guard local information ? At present, we did not see any solution to this problem. We would have liked to migrate code. And we would have liked to Program/train a recipient machine "on the job", as is done in the Japanese TRON system. But we did not see any sound possibility to overcome the risks involved. So we had to refrain from code migration. Again, we put

control back in the hand of the owner of the local machine. Using the "NetWork Processor" demon, the onwer may set up one trusted path, and only programs in this trusted path will be accessed by NetWork. So we rely on the risk awareness of the owner, and the usual local system provided by the file system access privileges. To educate user awareness, we took the aggressive way. We gave an example of how you can risk everything by putting an unrestricted shell in the trusted path. And we told everyone to take a lesson from it and never to do this.

(3) Competing access. This is an issue which was not addressed in D.H. Lawrence's letter. But we felt it of utter importance. If you have a distributed computing system, it will compete for network bandwith. Moreover probing and look-up will generate computing load even on those stations which are not used for idle time computing. In particular, any machine must be handle every broadcast it sees, even just to discard it. Competing communication load will be negligible for small sites. But it may become a major problem if the number of compute clients increases. If a distributed computing system does not address these problems, mere communication load may lead to a denial of service with increasing system size. NetWork takes three means to address this problem. (A) instead of using high overhead protocols like RPC, we use lightweight communcation for UNIX, based on UDP - and have special techniques to reduce communication load, (B) we limit the additional bandwith taken up by the NetWork administrative system to an arbitrary fraction (1 per cent) of the bandwidth on the transport medium available, (C) we control and limit the global rate of broadcasts and multicasts used by NetWork.

G. Sawitzki <gs@statlab.uni-heidelberg.de>

### Kisks in book buying -- shareware

Bill Putnam <billp@ivy.isc.com> <billp> Mon, 10 Feb 92 15:41:28 -0800

The following was reposted to comp.text from an original BIX newsgroup (ibm.utils/onions???). This is the first time I'd heard of such an elaborate scheme associated with shareware. I have not looked at the book yet, myself (perhaps I should be fore submitting a real posting to comp.risks), but even if the story is inaccurate, it bears passing on because it points out yet another possibility in mistruth-in-advertising.

In article <52928@cup.portal.com>, Lynlee@cup.portal.com (Linda Stefny Baum) writes:

- > From: Lynlee@cup.portal.com (Linda Stefny Baum)
- > Subject: Beware the THOUSAND DOLLAR BOOK.
- > Date: Fri, 17 Jan 92 17:07:10 PST
- > Organization: The Portal System (TM)
- >
- > The author of the following article has allowed me to repost his article IF
- > I did NOT post his name with it.. He is a BIX user.. The article was posted
- > to BIX. The Header info is complete with the exception of the authors name.
- >

> TINAR = This is NOT a Review.. > ibm.utils/onions #4290, from -----, 1245 chars, Mon Dec 30 00:45:24 1991 > There is/are comment(s) on this message. > -----> > TITLE: Beware the THOUSAND DOLLAR BOOK. (TINAR) > > "DOS Power Tools, Second Edition" looks a lot like the First Edition. The > price is \$10 higher, but, why not? The first edition only had one disk, > containing a lot of useful, ready to run, PAID FOR, utilities, at \$39.95. > This one's got THREE disks filled with "over 100 all-new utilties", at \$49.95. > > I've had the book for a week, and I'm reading page 811. This is where the > author urges you to register shareware you use; it's the right thing to do. > Sounds beautiful so far, what makes this an ONION? > > > MOST OF the "100 ALL-NEW UTILITIES" with this \$49.95 book are SHAREWARE! > 48 programs, by 7 authors, asking for a total of \$925 in registration fees! > 18 additional programs ask to "call or write" to 5 more authors for prices. > If each "write for price" is only \$25, the grand total is \$1,375. Even if I > pay each author for ONE program, the total registrations would come to \$242. > > On the covers, there's NO notice of the \$1,375 shareware bargain inside. > This important information is on page 815 thru 965 of this 1070 page book. > > Bantam Computer Books, ISBN 0-553-35464-7. Down payment only \$49.95. > Total price approximately \$1,424.95. Postage and taxes not included. TINAR. > > > Personally speaking, I feel this type of practice, if not illegal, is > unethical.. The first edition did not require the purchaser of the book to > pay large sums for the use of the Shareware included.. There was an > agreement with the publisher and the shareware authors For which, Im certain, > the authors were compensated for their labors.. I, for one, will not support > this type of tactic.... TINAR Lynlee@cup.portal.com >

I agree with Linda, hence my forwarding this to comp.risks. Caveat Emptor and don't let them get away with it when despite your best efforts to prevent being taken, you are.

Bill Putnam, INTERACTIVE Systems, 26635 W. Agoura Rd., Calabasas, CA 91302 A Kodak Company uunet!isc!ism!billp 818/880-1200 x2119

#### Prescription drug plan "benefits"

Jim Purtilo <purtilo@cs.UMD.EDU> Mon, 10 Feb 92 09:41:59 -0500 I recently needed to use my "prescription drug plan" employee benefits, available to Maryland state employees. (This is in response to problems with a flu virus rather than computer virus, as usually discussed in this forum.) This presented my fever-ridden imagination with an interesting array of risks due to a system that is substantially supported by computer.

The prescription drug plan in Maryland is contracted out to a separate company called PCS, Inc. Our membership ID is, unfortunately, assigned by social security number. All transactions in the system are recorded in a "PCS databank", a centralized facility that is billed as being an important employee safeguard, since it is intended to warn pharmacists when you are given some conflicting medications. The obvious sorts of computer risks here have been discussed previously -- what if the databases' list of drug interactions is not correctly recorded, what if the data being entered for a patient is misentered or associated with another patient, etc.

But the fine print in our benefits contract reveals there is room for other sorts of problems. We aren't given much in the way of promises concerning accuracy of information ("... neither PCS nor your ... sponsor is responsible for any damage or liability out of or in connection with the performance, or failure to perform, ... services for you.") Neither are we given much in the way of assurance concerning how information is to be used. Is PCS free to decide someday to sell mailing lists based upon records? Or (more likely) sanitized records? Send all those heart patients advertisements for the latest Ronco CPR-o-matic! (And what if they mix it up and send diabetics those chocolate ads really intended for folks with eating disorders....?) A longer range issue, of course, is that this is one more way for the state to get access to personal medical information. Want to custom-tailor a benefits package to the employee? No problem --- just tap into the centralized medical records and see what kinds of problems they'll likely have down the line. (Let's see, this Purtilo guy is overweight, attitude-ridden and near-sighted... better charge him the max for medical insurance. Now if we could only cross reference the DNA mapping info in order to predict other diseases....) Entry into this database is mandatory for any employee who uses the plan benefits.

This assumes you can use the benefits. The cough syrup I wanted to buy took about 40 minutes to prepare. 10 of these minutes were due to waiting in line and paperwork, 30 were due to the lab person fooling around at the computer terminal. The pharamacist was not very open to gab about this, so I cannot report on his perceptions concerning system reliability, but I got the distinct impression that if they could not log in to the centralized facility, then I could not buy the medication (under the plan). Moreover, since membership cards are only issued in the employee's name, it is plausible that a valid user might \_not\_ get medication at all: spouse goes with prescription and no cash, expecting to get critical prescription filled under terms of the plan; computer is down, denying verification of user [the card explicitly states that only the user whose name is on the card can get benefits ... participating pharmacies are told to overcome this problem for family members by checking in the computer]; spouse has different last name than on card, so the pharmacy cannot even honor the card based upon paper records; and spouse doesn't have the cash to buy the medication (and hope the paperwork doesn't kill him or her later).

Jim (purtilo@cs.umd.edu)

# Re: Radiation underdoses

Jon Jacky <JON@gaffer.radonc.washington.edu> Mon, 10 Feb 1992 10:52:27 -0800 (PST)

All I know about the recently reported radiation therapy underdoses are what I read in RISKS. As usual, it is not possible to determine what actually happened from the news account.

However, since I do work in a radiation therapy clinic, I can provide some general information.

Doctors prescribe the radiation dose that is to be delivered to particular sites in the patient's body. Typically the prescription includes, in effect, a lower limit on the dose to the tumor and an upper limit on the dose to various healthy tissues such as the spinal cord, etc. Then a physicist or dosimetrist creates a treatment plan, including a geometric configuration of radiation sources (usually beams from a linear accelerator), and the amount of radiation to be delivered from each source. Because of the nature of the radiation producing machinery, and the physics of radiation absorption in the body, physics calculations are required to determine the machine settings needed to deliver the prescribed doses to the prescribed sites.

Clinic staff usually use computer programs called "treatment planning programs" to perform some of these calculations. Usually, these programs produce a printed chart with instructions for setting up the treatment machines, including the total quantity of radiation to be delivered. The treatment planning computer system is usually a completely separate system from the therapy machines. Usually the information from the planning program must be manually entered into the control console for the therapy machine (whether or not the therapy machine itself is computer-controlled). Recently some vendors have produced treatment planning systems that allow some calculated machine setup information to be loaded directly into a (computer-controlled) treatment machine via some kind of network connection.

All treatment planning programs depend on tables of data representing actual machine characteristics measured at the clinic. Clinic staff must measure this data and enter it into tables in the format required by the planning program. These days, the data is often collected with the aid of a semi-automated "beam scanner" that includes a small computer. This system is usually completely separate from both the therapy machine and the treatment planning system. Sometimes there are facilities for loading data from the scanner into the planning system via network, without having to type it in manually.

In addition, the therapy machines themselves have calibrations that must be adjusted frequently by clinic staff. On some of the newer computer-controlled machines, a computer is involved in this process as well.

Besides the therapy machine, the treatment planning system, and the beam scanner, clinics have other instruments that are used to calibrate the rest.

I hope I have conveyed that there are many steps and stages where the clinic

staff have the obligation to measure, record and update information that must be accurate and consistent. Computing is involved in many of these stages. There are many opportunites for errors, in particular there are many opportunities for dose delivery errors other than the therapy machine itself. Clinics must have quality assurance procedures in place to detect and correct the errors that do occur before they can affect patients. To me, the most alarming aspect of this recent story is that some kind of error was apparently allowed to remain uncorrected for years.

One thing that is important to understand is that many clinics do not depend solely on stock equipment from vendors; some use quite elaborate procedures and instruments that are custom built by clinic staff. As part of this tradition, it has long been common to use custom computer programs written by clinic staff for treatment planning and other tasks. Many clinics that own and use commercially produced treatment planning systems and beam scanners also use locally-written programs for some special applications, or to act as pre-processors, post-processors or interfaces between purchased programs. Moreover, almost all commercial offerings are actually adaptations of systems that were originally developed by staff at some clinic to meet some local need.

Quite often there is no clear distinction between "the physicist" or "the expert" and "the programmer". Many people who develop software that is used in radiation therapy clinics (including yours truly) also have clinical service duties, and their formal education often does not include specialization in computer science or software engineering. I don't believe this is necessarily a bad thing, but I think it is fair to say that the quality of the methods used and of the resulting products varies a great deal.

- Jonathan Jacky, Department of Radiation Oncology, University of Washington

# ✓ System certification again (Re: Radiotherapy, Randell/PGN, RISKS-13.12)

Rick Smith <smith@SCTC.COM> Mon, 10 Feb 92 14:48:30 CST

> [The Therac 25 case was one of OVERdoses being life critical.

> It is appropriate to note that UNDERdoses may also be life critical. PGN]

If a machine is expected to do it \_right\_ then people should have a way of monitoring whether or not the machine did it right. There should be some way of measuring what the machine is doing while it takes place. They could monitor the radiation and keep a record of what the patient actually received.

These machines should be subjected to routine measurements and calibration checks to insure that they're doing what they should. The state department of weights and measures goes around and verifies that gas pumps and grocery scales are accurate. Shouldn't we expect that hospitals could do the same to their radiation machines?

Any museum worth its salt has thermographs and humidigraphs all over the place, recording on paper the temperature and humidity next to their valuable relics. I'm sure that all of these buildings have central heat/AC/climate control. But they stil use separate measuring tools to verify the results of the automatic systems.

Perhaps we're just seeing the "black box to solve all your problems" mentality in the buyers of these automated radiation machines. Or else it's another case of cost containment.

Rick Smith, SCTC, Arden Hills, Minnesota.

# ✓ Software Engineering licensing again (Radiotherapy, Tyzuk, <u>RISKS-13.13</u>)

Marc Horowitz <marc@Athena.MIT.EDU> Sun, 09 Feb 92 01:25:57 EST

<> With regard to computer risks in general: <> I think it is time to establish licensing of software engineers, ...

Is it a meta-RISK that making such a controversial recommendation (which has been beaten into the ground before) to such a large audience is likely to flood PGN with responses to the point where he's likely to ignore all of them?

Marc

# Software Engineering licensing again (Radiotherapy, Tyzuk, <u>RISKS-13.13</u>)

Perry E. Metzger <pmetzger@shearson.com> Tue, 11 Feb 92 13:45:13 EST

> I think it is time to establish licensing of software engineers,...

I strongly disagree.

Licensure of most professions exists not to protect the public, but to restrict entry into a field so as to artificially protect the wages of the professionals belonging to the newly-formed guild. This concept of licensure goes back to medieval times. One would think that we had advanced beyond feudal times, but it appears that we have not. A recent cause celebre in Washington, DC has been a hair salon fighting the districts strict cosmetologist licensing laws. You heard me: licenses are required to style hair in Washington. The AMA has, via its legal right to control accreditation of medical schools and licensure of physicians, systematically reduced the supply of Doctors in our country, thus driving up the price of health care. Lawyers manage every day to drive anyone who is willing to help people fill out simple legal forms out of business with lovely laws about practicing law without a license.

All of this is silly. There is little or no evidence that licensure does anything other than creating a new protected class of people who can jack up their fees arbitrarily because they can restrict entry into their field. No studies or statistics exist to show that people get better lawyers, cosmetologists, or even physicians, thanks to licensing laws. However, in the absence of any substantive evidence for quality improvements in the presense of licensure, people anxious to run the lives of other people add hundreds of new protected classes of people every year. Recently, the state of New Jersey created a new protected class of food specialists. No one but a licensed dietitian can pronounce your carrots nutritious these days; anyone else giving out "dietary advice" can get their fannies whacked by the long arm of the state licensing board.

Even if government licensing could increase safety, the costs involved would have to be considered. Just as safety could be enhanced by forcing all cars to travel under 10 MPH, but needed productive uses of automobiles would then be eliminated, government licensing could drastically increase the costs of software development without a commensurate improvement in safety.

Government is a fearsome weapon, and rarely a useful tool. I think of it in the "guilty until proven innocent" category. Until someone can present clear and sound evidence that licensure of software engineers has actually dropped the number of dangerous product failures, without incurring excessive costs to society, I will oppose the concept.

Perry Metzger

# Software Engineering licensing again (Radiotherapy, Tyzuk, <u>RISKS-13.13</u>)

Rich Kulawiec <rsk@gynko.circ.upenn.edu> Wed, 12 Feb 92 23:17:28 EST

>I think it is time to establish licensing of software engineers,...

I might agree with this in theory, but want to point out that licensing and review boards are not silver bullets, to borrow a phrase from Fred Brooks' recent article in "Computer".

The history of civil/mechanical/electrical engineering is replete with examples of disastrous projects designed by appropriately trained and licensed engineers, and approved by suitably experienced review boards. I'm not sure the situation would be any different for software engineering; we just might feel better about the issue if licensing and boards existed.

>Many programmers of such systems have no knowledge whatsoever of the techniques >of reliable programming. They were the scientist, or expert, or whatever on the >object under software control, and were chosen to write the program because >they could hack out something that worked.

Sometimes they're chosen because they're the only person available who understands the entire task at hand. I wrote some of the firmware that controls the X-ray tube gantry in the Omnimedical Quad-One CT scanner; I was selected because I understood something about X-ray tubes, stepper motors, power control circuitry, real-time software, 6809 assembler, sliding-ring mechanics, and gate-level TTL circuit design. A person with a better background in software engineering almost certainly would have written better code -- but they may not have understood the electromechanical aspects of the system as well as I did.

>Consequently, they turn out spaghetti.

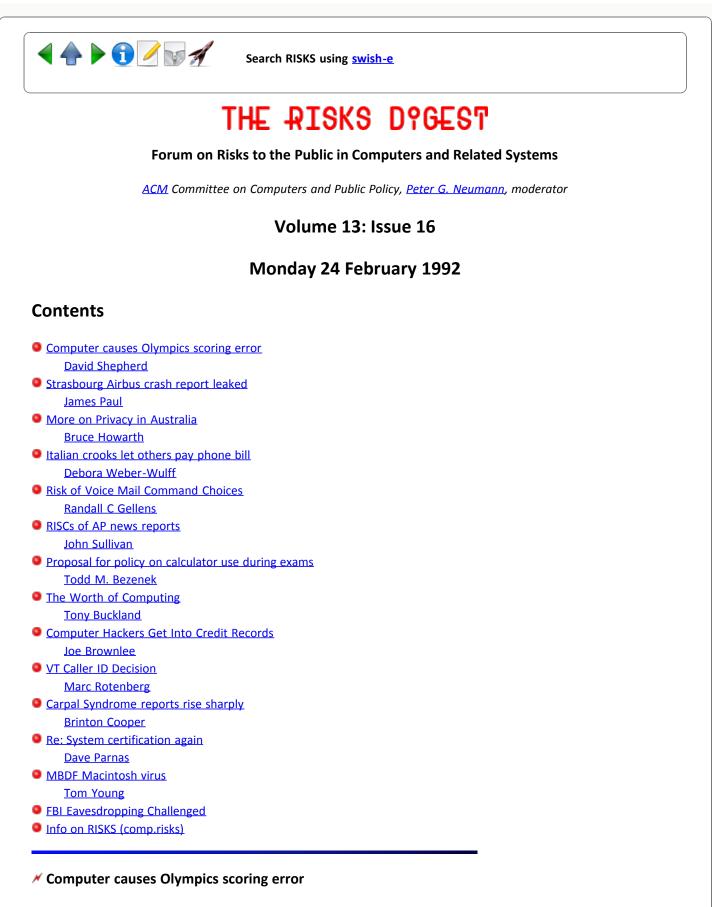
Well, sometimes they turn out spaghetti, and sometimes they do a pretty good job of organizing the code into something that's robust, testable, and maintainable. But "they" may turn out to be software engineering graduates or medical physics specialists -- and it's hard to tell which by looking at their code.

---Rsk rsk@gynko.circ.upenn.edu Cardiothoracic Imaging Research Center



Search RISKS using swish-e

Report problems with the web pages to the maintainer



David Shepherd <des@inmos.com> Fri, 21 Feb 92 16:52:27 GMT During the first session of the women's ice skating competition, the UKs number 1 skater, Joanne Conway, complained of biased scoring after the Canadian judge gave her only 4.2 marks while all the other judges gave around 5.0 to 5.5. Subsequently the Canadian judge has revealed that she intended to give 5.2 marks. Each possible score has a separate button to press to signal the score to the computerized scoring system. By mistake the judge pressed 4.2 instead of 5.2 and, even though she realized her mistake, there was no provision to correct the mark. The only way of correcting it would have been for the UK team to lodge an official appeal - which wasn't considered worthwhile as it was only the difference between 17th and 15th place.

In another incident the UK 2 man bob team, in the lead at that stage, went out of contention after being kept at the start of 7 minutes while one of the intermediate timing controls was fixed - note that this timer was not needed for the actual result, just to give an intermediate split time. Perhaps another indication of where technology becomes the master rather than the servant of sport. (Some people have tried to read a more sinister implication of a Swiss engineer holding the leading team up for 7 minutes which help the Swiss No 1 bob go into the lead!)

david shepherd: des@inmos.co.uk or des@inmos.com tel: 0454-616616 x 625 inmos ltd, 1000 aztec west, almondsbury, bristol, bs12 4sq

[The old Swisseroo? Bobbing for Apples (if they were using a Mac)? The "Unified" team now has to settle for good marks and Lennon music. Next time someone will figure out how to hack into the scoring computers.

I wondered on several very obviously partisan judge's scorings, with outrageous (+/- outlier/outliar) scores, whether the judge was overtly trying to cheat ... I thought they used to discount the highest and the lowest scores on judged events, but apparently not. PGN]

## Strasbourg Airbus crash report leaked

James Paul, U.S. House Science Committee <"NOVA::PAUL"@yttrium.house.gov> Fri, 21 Feb 1992 10:46:30 -0500 (EST)

### AIRBUS CRASH PROBE CITES HUMAN, TECHNICAL ERROR

PARIS, Feb 20, Reuters - French television said on Thursday a preliminary report to be published next week on the causes of last month's Airbus A320 crash which killed 87 people did not blame the disaster on any single factor or person. The TF-1 channel said the independent commission's report concluded that a mixture of human and technical error had caused the Air Inter flight from Strasbourg to Lyon to plough into a snow-covered mountainside on January 20, just five minutes before it was scheduled to land. Nine people survived. TF-1 said the commission's findings showed the Strasbourg airport was not equipped with landing approach systems matched to the sophistication of the Airbus, and that there were serious failings in the crash plane's altimeter system. The commission concluded the pilot either did not know how or was unable to stop the plane's abnormally rapid descent, according to TF-1. The station did not reveal how it gained access to the report. Publication of the report was delayed because Transport Minister Paul Quiles is visiting Portugal on Friday and wants to study the findings before commenting.

The French civil aviation authority has already taken some preliminary measures, urging all airlines flying the A320 to review their procedures for using the VOR-DME beacon system for landing. But the authorities decided against grounding the planes, saying there was no initial evidence that mechanical problems caused the disaster.

National carriers Air France and Air Inter earlier this month banned their pilots from using the automatic landing procedure until further notice.

A spokeswoman for Toulouse-based Airbus Industrie said earlier the aircraft maker did not yet have a copy of the report and would have no comment until it did. Meanwhile a judge investigating legal responsibility for the crash staged a reconstruction flight on Thursday, circling the accident site three times.

### More on Privacy in Australia

<bruce@socs.uts.edu.au> Wed, 19 Feb 92 08:55:55 EST

[RISKS-13.14 included "Australian Government Bungles Private Data". Bruce submitted the article "DSS blames printer restart for bungle", by John Hilvert, in Computerworld Australia, 14 Feb 1992, omitted here. That article supports the printer-restart synchronization glitch theory. PGN]

By one of \*those\* coincidences, it was reported on TV the same week that a branch of the Australian Taxation Office (ATO) sent similarly misprinted forms to some (as I recall, 80) taxpayers. Two of the taxpayers had contacted each other, then presumably the media, to share their disgust at the release of income and savings data. An ATO employee on the TV claimed that the misprints had been caused by a folded page in a box of paper.

Bruce Howarth, Uni of Technology Sydney

### Italian crooks let others pay phone bill

Debora Weber-Wulff <weberwu@inf.fu-berlin.de> Sat, 22 Feb 1992 12:54:43 GMT

[Translated by DWW from the Berlin daily Newspaper "Tagespiegel", 22 Feb 1992]

lui, Rome, 21. February 1992. [...] Half a million Italians are the proud owners of portable telephones. The cordless appliance has become the favorite toy of the Southerners, but the game may soon be over: the "telefonini" are not protected.

Under the motto "Buy one, pay for two", crooks sell manipulated phones that are used so that the buyer has to pay for the toll calls of the seller. The trick works like this: the crooks take a computer with a computing program [whatever that is ;-) dww] like the ones uses to crack automatic teller machines, and fuss with it until they find the secret code for the telephone. The code is a

combination of the telephone number and the serial number that is supposed to only be available to the telephone company SIP. When the code has been cracked, it is no problem to transfer it to a second telephone, so that both telephones have the same license number. One phone is sold "under the hand" by the crooks. As an added deal, the buyer not only gets to pay his own phone bill, but the fees run up on the second phone as well. The Italian underworld is especially keen on using this method.[...] The mafia uses the "portabili" for conducting their unclean business.

[... The police] have not been able to find the instigators, but they suspect that employees of the telephone manufacturing company are involved, as they have the knowledge of how the phones are constructed. [...] The portable telephone is well-known for the ease of tapping the telephone conversations [which cannot, however, be traced to the place of origin. A book calle "Italy, I hear you calling" with some of the more interesting tapped conversations has just been published.]

[Why is such a telephone easy to crack and easy to reprogram? dww]

Debora Weber-Wulff, Institut fuer Informatik, Nestorstr. 8-9, D-W-1000 Berlin 31 +49 30 89691 124 dww@inf.fu-berlin.de

### Kisk of Voice Mail Command Choices

Randall C Gellens <0005000102@mcimail.com> Wed, 19 Feb 92 09:15 GMT

[I sent this as a reply to Telecom. It's probably not a serious enough risk to go into Risks, but I thought I'd let you decide. --Randy]

In TELECOM Digest Volume 12 : Issue 108, the moderator (Patrick A. Townson) discusses Ameritech Voice Mail Commands and Security Flaws:

> After the message has played out, 5 to delete it; 7 to save it.

Considering that the Aspen voice mail product (from Octel,I think) uses 7 to delete a message, and that Aspen is widely used by businesses, this seems an unfortunate choice, as people with Aspen at work and IBT RVMS at home will be likely to confuse 7 and end up deleting messages by accident. Of course, this is not as serious a risk of nonstandardization as airline flight controls which differ from model to model :-).

--Randy

## RISCs of AP news reports

<sullivan@geom.umn.edu> Mon, 24 Feb 1992 10:55:18 -0600

An Associated Press article on new processor chips announced at the International Solid State Circuits Conference appeared in the (Minneapolis) Star Tribune last Thursday. It says, in the middle: Most of the chips use a technology called reduced instruction set computing (RISC), which speeds the processing of data by limiting the number of instructions the processor must execute. The microprocessors that power personal computers, by contrast, use a different technology.

Of course, limiting the number of instructions a processor knows how to execute typically increases the number of instructions it must execute.

The Op-Ed page of The New York Times yesterday (Feb 23) has an essay by David Gelernter from Yale's CS dept complaining that when newspapers (even The Times) use the term "operating system", they feel obliged to define it. But someone who doesn't know what one is is "not going to learn on the basis of a single phrase, no matter how artfully crafted".

He doesn't mention how misleading a single phrase can be, if crafted by a reporter who doesn't know technology.

-John Sullivan, Sullivan@Geom.UMN.Edu

## proposal for policy on calculator use during exams

Todd M. Bezenek KOON <plains!bezenek@uunet.uu.net> 21 Feb 92 07:01:23 GMT

[This is an article which I recently posted to comp.sys.handhelds and comp.sys.hp48. It is in response to a discussion regarding the use of calculators on university exams. I am posting it to comp.risks because it demonstrates the risk of introducing computing power into the classroom where it may be misused. TMB]

I have reviewed the responses concerning calculator policies at universities from all over the world. Thank you to everyone for sending them. The following is my proposed policy. This policy is intended to eliminate problems associated with using note-style information, without eliminating the use of the calculating power of these devices. If you have any comments, please post them after thinking them through fully.

Proposed Policy Regarding the Use of Portable Calculating Devices during Closed-Note Examinations

If a student uses a portable calculating device during a closed-note examination for the purpose of storing notes, that student shall be considered guilty of an infraction equivalent to using said notes as they would appear on paper.

In the case that a proctor believes beyond a reasonable doubt that a student is violating the above policy, that proctor shall immediately remove the calculating device from the student's possession. The proctor may then choose whether or not the student should be allowed to complete the examination. The calculating device shall remain in the possession of the proctor until the contents of its memory--both vendor supplied and user programmed--can be examined.

The decision of whether or not the above policy has been violated should be based upon the judgement of a faculty member who shall examine the memory of the calculating device before it is returned to the student. In the case that the memory is found to contain information which, when transferred to paper, would be considered an unallowable aid, the student shall be considered guilty of the infraction described above.

In the case that the student is found to not be in violation of the above infraction, the student should be allowed to rewrite the examination if the student so chooses. Alternately, if the student is found to be in violation, the student is subject to the same university policies that govern the use of unallowed notes equivalent to that which would result from transferring the memory of the calculating device to paper.

In no case will the student forfeit possession of the calculating device indefinitely.

Respectfully submitted, Todd M. Bezenek

Todd Michael Bezenek, KOONInternet: bezenek@plains.nodak.eduUUCP: uunet!plains!bezenekBitnet: bezenek@plains

## The Worth of Computing

Tony Buckland <buckland@ucs.ubc.ca> 24 Feb 92 15:04 -0800

>From @yonge.csri.toronto.edu:msb@sq.sq.com Mon Feb 24 14:50:45 1992

You write in can.general:

- > Yesterday, thieves broke into a VanCity Savings branch and stole
- > two bags from a night deposit box. But not to worry unless
- > you're in the computing game and proud of it " ... all they
- > got were worthless computer printouts and administration documents."

Mark Brader, Toronto, utzoo!sq!msb, msb@sq.com

### Computer Hackers Get Into Credit Records

<joe@cbquest.att.com> 20 Feb 1992 7:15 EST

>From the Columbus, Ohio, \_Dispatch\_. Any typos are mine.

Computer Hackers Get Into Private Credit Records

DAYTON - Computer hackers obtained confidential credit reports of Midwest consumers from a credit reporting firm in Atlanta. Atlanta-based Equifax said a ring of 30 hackers in Dayton [Ohio] stole credit card numbers and bill-paying histories of the consumers by using an Equifax customer's password.

Ronald J. Horst, security consultant for the company said the break-in apparently began in January. Police don't know if the password was stolen or if an employee of the client company cooperated with the hackers. Horst said the hackers were apparently doing it just for fun. No charges have been filed. Equifax will notify customers whose credit reports were taken.

#### [End of quotation]

The usual caveats about media reporting of computer-related topics apply here. One thing I don't like about this article is the implication that since the hackers were doing this for "fun", they won't be prosecuted. Of course, the article doesn't say that exactly, but I'll be watching to see if this case goes any farther.

I'll also be waiting to see of I'm one of those people whose credit reports were stolen, and, if so, what Equifax intends to do about it other than to notify me.

Joe Brownlee, Analysts International Corp. @ AT&T Network Systems, 471 E Broad St, Suite 2001, Columbus, Ohio 43215 (614) 860-7461 joe@cbquest.att.com

# VT Caller ID Decision

Marc Rotenberg <Marc\_Rotenberg@washofc.cpsr.org> Wed, 19 Feb 92 11:59:52 PST

### VT Caller ID Decision

The Vermont Public Service Board has just released its Caller ID decision. It's good result with an interesting new wrinkle.

Vermont will require that New England Telephone (NET) make free, per-call blocking available to all subscribers. NET will also be required to provide free, per-line blocking to all subscribers with non-published telephone numbers. And NET will be required to provide free, per-line blocking to all subscribers who have "a legitimate concern that it would be unsafe to transmit" their telephone numbers, including clients, volunteers and staff associated with domestic violence and sexual assault agencies.

The Hearing Officer initially recommended that such requests should be subject to review by NET, but the Public Service Board rejected this approach. The Board ruled that all customers should be entitled to receive free per-line blocking through a "simple declaration."

The Vermont Public Service Board thus found a clever solution to a difficult problem that was first identified in the Pennsylvania Caller ID case. In that case, as in Vermont, concern was expressed that certain individuals may require blocking to maintain personal safety. But the Bell company's proposed "certification procedure" left it unclear as to who would qualify for privacy protection or how adverse decisions could be appealed.

For these reasons, the Pennsylvania court held that the certification procedure

violated basic due process rights. (The Pennsylvania court also found that Caller ID violated the state wiretap statute and the state constitutional right of privacy and ruled that the service could not be offered in the state).

The due process problem -- deciding who is entitled to greater privacy protection and who gets to makes the decision -- remains one of the most interesting and difficult issues in the Caller ID debate.

In ruling that phone subscribers should be entitled to decide for themselves whether per-line blocking is appropriate, Vermont has avoided the due process problem that arose in Pennsylvania.

In the Vermont proceeding, CPSR was asked to serve as the Board's expert witness after the Board determined that "there existed a serious imbalance in the respective parties' ability to present evidence on all relevant issues."

New England Telephone then retained Harvard Law School Professor and Legal Affairs TV Commentator Arthur Miller as their expert. Professor Miller had earlier stated that Caller ID should be offered without blocking, but in this case acknowledged that per-call blocking might be an appropriate solution.

CPSR provided extensive testimony for the Vermont Public Service Board on the privacy implications of Caller ID after carefully reviewing concerns expressed by those affiliated with domestic violence shelters in the state.

Marc Rotenberg, CPSR Washington Office

## Carpal Syndrome reports rise sharply (Helgesen, <u>RISKS-13.14</u>)

Brinton Cooper <abc@BRL.MIL> Wed, 19 Feb 92 16:26:07 EST

Jeff Helgesen relates a Chicago Tribune article on the sharp increase in Carpal Tunnel Syndrome (repetitive-motion disorder) and the discussion about high-risk workplace environments. The article said, in part,

When someone applies force over and over to the same group of muscles, the same joint or the tendon, the result may be tissue tears and trauma. Other factors causing damage are awkward joint posture and prolonged constrained posture.

I have no doubt that this is true as stated. However, anecdotal evidence causes me to wonder if we're missing something. (I emphasize that this is anecdotal.) Every sufferer of carpal tunnel of whom I am personally aware is a cashier at a supermarket. Yet, I work in a laboratory where some very intensive computing activity takes place. We have people who frequently spend more than 10 hours out of 24 at keyboards. I am unaware of any carpal tunnel cases here (although I admit the possibility). This causes me to wonder:

What part does psychological or emotional stress play in the development of repetitive-motion disorders?

Supermarket cashiers do the work largely for the money. Folks at this lab work here for the same reason, but there is great job satisfaction, (dare I call it "fun?") here that doesn't exist at the grocery store. Does it matter?

(It's no less a risk either way, but it's better to understand the risk as much as possible.)

Brint

[By the way, apologies for losing Elizabeth Willey's contribution in <u>RISKS-13.15</u>. She pointed out that there are lots of parts of the body that can suffer from repetitive motion syndromes, not just the carpal tunnel areas. Somehow her message got lost. Sorry. PGN

# Re: System certification again (<u>RISKS-13.15</u>)

Dave Parnas <parnas@triose.eng.McMaster.CA> Wed, 19 Feb 92 08:45:28 EST

Marc Horowitz was correct and Perry E. Metzger and Rich Kulawiec, with the support of Peter Neumann, proved him correct.

Dave

## MBDF Macintosh virus

Tom Young <xmu@piccolo.cit.cornell.edu> Fri, 21 Feb 92 23:20:10 GMT

(This is being posted on behalf of M. Stuart Lynn)

As I am sure you are aware, a new Macintosh virus, MBDF-A, has been detected in the Info-Mac archives at SUMEX-AIM that has also been mirrored to other archives. Furthermore, it appears that the virus may have originated from or have been vectored through a machine at Cornell.

Other folks are addressing issues of detection, elimination, and prevention. I just want you to know that we at Cornell take this situation most seriously, and are doing everything we can to track down the origin and the originator of this virus. The university absolutely deplores this kind of behavior, and should it indeed prove that the originator was a member of this community we will pursue all appropriate remedies under our computer abuse policy.

If anyone out there has any relevant technical information that would help us track down the originator, I would appreciate it if you would send it to Tom Young (XMU@cornellc.cit.cornell.edu).

M. Stuart Lynn, Vice President for Information Technologies, Cornell University 607-255-7445

[Also posted to RISKS by laurie@piccolo.cit.cornell.edu (Laurie Collinsworth)]

## FBI Eavesdropping Challenged

<[anonymous]> Tue, 18 Feb 92 10:01:34 PST

FBI Eavesdropping Challenged WASHINGTON (AP, 17 Feb 1992)

Cellular telephones and other state-of-the art telecommunications technology are seriously challenging the FBI's ability to listen to the telephone conversations of criminal suspects, law enforcement officials say. The FBI is seeking \$26.6 million next year to update its eavesdropping techniques. Normally tight-lipped FBI officials become even more closed-mouthed when the subject of investigative "sources and methods" comes up. But a review of the bureau's 1993 budget request provides an unusual glimpse into the FBI's research on electronic surveillance and its concerns about new technologies.

"Law enforcement is playing catchup with the telecommunications industry's migration to this technology," said the FBI's budget proposal to Congress. "If electronic surveillance is to remain available as a law enforcement tool, hardware and software supporting it must be developed."

The new technologies include digital signals and cellular telephones. At the same time, there has been an increase in over-the-phone transmission of computer data, which can be encrypted through readily available software programs, say industry experts and government officials.

The FBI's five-year research effort to develop equipment compatible with digital phone systems is expected to cost \$82 million, according to administration figures.

The FBI effort is just a part of a wider research program also financed by the Pentagon's secret intelligence budget, said officials who spoke on condition of anonymity.

Electronic surveillance, which includes both telephone wiretaps and microphones hidden in places frequented by criminal suspects, is a key tool for investigating drug traffickers as well as white-collar and organized crime.

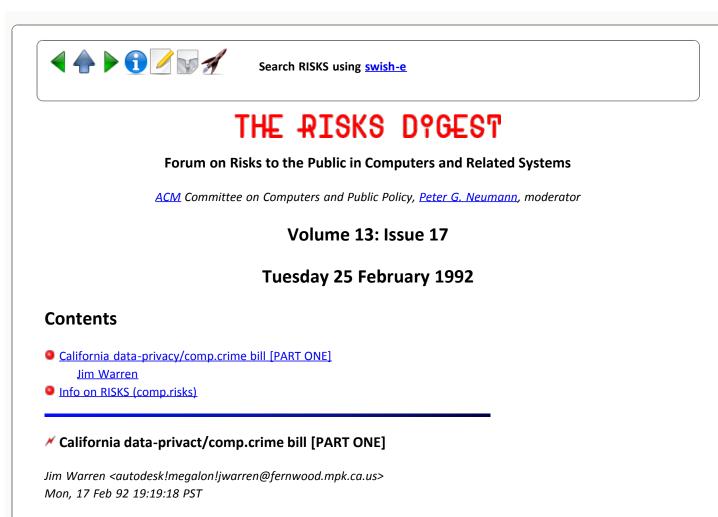
Conversations recorded by microphones the FBI placed in the New York City hangouts of the Gambino crime family are the centerpiece of the government's case against reputed mob boss John Gotti, now on trial for ordering the murder of his predecessor, Paul Castellano.

Taps on the phones of defense consultants provided key evidence in the Justice Department's long running investigation of Pentagon procurement fraud, dubbed "Operation III Wind." But with the advent of digital phone signals, it is difficult to unscramble a single conversation from the thousands that are transmitted simultaneously with computer generated data and images, industry officials said.

"In the old days all you had to do was take a pair of clip leads and a head set, put it on the right terminal and you could listen to the conversation," said James Sylvester, an official of Bell Atlantic Network Services Inc. But digital signal transmission makes this task much more difficult. Conversations are broken into an incoherent stream of digits and put back together again at the other end of the line.

John D. Podesta, a former counsel to the Senate Judiciary's law and technology subcommittee, said the FBI and other law enforcement agencies are simply victims of a technological revolution. For more than 50 years the basic telephone technology remained the same.





This includes the full text of legislation that was introduced Feb. 10th in the California State Senate by a senior member of that body, the Chair of the Senate Judiciary Committee, Senator Bill Lockyer of Southern Alameda County. This copy of the bill plus staff background comments is being uploaded within days of its availability in Senate offices.

SB1447 TOPICS

Sec.1: "Privacy Act of 1992", Senate Bill 1447 (Lockyer, Privacy)

Sec.2: Driver's licenses: Use of human-readable and magstripe information

Sec.3: Privacy: Rights of employees and prospective employees

Sec.4: Computer crime laws: Modifications

Sec.5: Automatic vehicle identification [AVI] systems: Control of uses

CONTENTS OF THIS CONTRIBUTION [words/chars]

[PART ONE -- <u>RISKS-13.17</u>]

Introductory comments and details of notation conventions [757/5191] Reformatted verbatim text of the Feb. 10th bill [3227/21285] [PART TWO -- RISKS-13.18]

Background notes prepared by Sen. Lockyer's assistant [2465/15546] [If printed, the entire contribution is approximately 12 pages.]

## **REPORTEDLY A LEGISLATIVE "FIRST"**

This effort in "electronic democracy" may be the first time that state legislation has been distributed online, for access by the general public, at the same time it becomes available to legislators and their staff.

A senior member of the Senate computer system's technical staff reportedly said they have never-before down-loaded a machine-readable copy of initial legislation onto a personal computer for redistribution on public computer networks.

Furthermore, Sen. Lockyer's Legislative Assistant responsible for the bill said he knows of no prior instance where legislative staff have gone online on public nets to seek citizen input and discussion about new legislation.

#### SOURCES OF ORIGINAL DOCUMENTS & INFORMATION

Mr. Ben Firschein is the Legislative Assistant to Sen. Lockyer who is handling this bill:

Office of Senator Bill Lockyer

Room 2032, State Capitol

Sacramento CA 95814

Mr. Firschein/916-445-6671, main number/916-445-5957, email/\*\* Formatted, binary, machine-readable versions of this text will be available on the WELL, the Whole Earth 'Lectronic Link. The WELL is a public teleconferencing system located in Sausalito, California, accessible via the Internet; voice/415-332-4335, 2400-baud data/7-E-1/415-332-6106. For readonly access instructions, SEND A REQUEST TO: jwarren@well.sf.ca.us. \*\* -- Mr. Firschein will be online on the WELL within a week or so. You may request his email address, also, from jwarren@well.sf.ca.us.

There will be four read-only files:

A. The original file that was down-loaded from the Senate's legislative computer system in WordPerfect format on a PC-compatible diskette.

B. The above file, converted to a Word-5.0 Macintosh format, with pagination approximating the printed copies of the bill available from the legislative offices.

C. Background information, explanations and mention of some alternatives, prepared by Mr. Firschein, in original WordPerfect format for PC-compatibles.

D. That backgrounder file, converted to Word-5.0 Macintosh format.

#### REPRESENTING LEGISLATION-IN-PROGRESS: A NOTATION PROBLEM

In the California Senate, printed legislation-in-progress uses the following conventions:

When stating new legislation, \*plain-text\* states PROPOSED law. When \*amending\* current law, \*plain-text\* states the CURRENT law, and \*strike-thru text\* indicates current law to be deleted while \*underscored\* or \*italicized\* text represents wording to be added to those current statutes. Deletions and additions represented by strike-thru and underlining or italics \*amend\* current law.

But, the basic ASCII character-set -- and a great many older terminals and computer printers -- have no strike-thru, italics or underlining. So, here is how that unavailable notation is represented in this document:

[[ annotation ]] -- explanatory comments by "uploader" Jim Warren all capitals -- originally bold-face text; no legislative meaning

Unless stated as amending current law:

plain-text -- text of new legislation, proposed to be new law When stated as amending current law:

plain-text -- text of current law to remain unchanged
<< strikethru <> -- text in current law, proposed for deletion
{{ underscore }} -- text proposed to be added to current law.

THE BEGINNING ...

The introduction of this legislation in the Senate is the beginning of a lengthy process or review and revision by amendment, prior to its possible passage into law.

Please send your comments and suggestions about the legislation -- and about the Senate staff's active cooperation in making it publicly available, online -- to Mr. Firschein and Sen. Lockyer.

--Jim Warren, 345 Swett Rd., Woodside CA 94062; voice/415-851-7075, fax/415-851-2814, email/jwarren@well.sf.ca.us -or- jwarren@autodesk.com [ for identification purposes, only: contributing editor, MicroTimes; Chair, First Conference on Computers, Freedom & Privacy (March, 1991); and member, Board of Directors, Autodesk, Inc.; blah blah blah ]

"THE PRIVACY ACT OF 1992" -- CALIFORNIA STATE SENATE BILL No. 1447 Introduced by Senator Lockyer February 10, 1992

An act to add Section 1799.4 to the Civil Code, to add Section 2805 to the Labor Code, to amend Section 502 of the Penal Code, and to amend Section 27565 of the Streets and Highways Code, relating to privacy.

### LEGISLATIVE COUNSEL'S DIGEST

[[\*\*\*\* The Legislative Counsel's Digest is NOT part of the bill. It is only a summary prepared by the legislature's legal counsel. \*\*\*\*]]

### SB 1447, as introduced, Lockyer. Privacy.

(1) Existing law prohibits the disclosure of specified information by business entities which perform bookkeeping services and by persons providing video cassette sales or rental services.

This bill would provide that a business entity that obtains information from a consumer's driver's license or identification card shall not sell the information or use it to advertise goods or services, without consent.

(2) Existing law prohibits employers from making or enforcing rules or policies forbidding or preventing employees from engaging or participating in politics, and from controlling the political activities or affiliations of employees.

This bill would provide that any employer shall be liable to an employee or prospective employee for damages caused by subjecting the employee to discipline or discharge, or denying employment to a prospective employee, on account of the exercise by that person of privacy rights guaranteed by the California Constitution.

(3) Existing law sets forth definitions and penalties for specified computer-related crimes.

This bill would require the owner or lessee of any computer, computer system, computer network, computer program, or data, as specified, to report to a local law enforcement agency any known violations of the provisions described above. The bill would also provide that any person who recklessly stores or maintains data in a manner which enables a person to commit acts leading to a felony conviction under the provisions described above, shall be liable to each injured party for a specified civil penalty. The bill would make related changes.

(4) Existing law requires the Department of Transportation to develop and adopt functional specifications and standards for an automatic vehicle identification system to be used in toll facilities, as specified.

This bill would provide that a vehicle owner shall have the choice of being billed after using the facility, or of prepaying tolls, in which case the department or any privately owned entity operating a toll facility shall issue an account number to the vehicle owner which is not derived from the vehicle owner's name, address, social security number, or specified other sources, and would prohibit the keeping of any record of this information.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

#### THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. This act shall be known and may be cited as the Privacy Act of 1992.

SEC. 2. Section 1799.4 is added to the Civil Code, to read:

1799.4. A business entity that obtains information from a consumer's driver's license or identification card for its business records or for other purposes shall not sell the information or use it to advertise goods or services, without the written consent of the consumer.

SEC. 3. Section 2805 is added to the Labor Code, to read:

2805. (a) Any employer, including any state or local governmental entity or instrumentality thereof, shall be liable to an employee or prospective employee for damages caused by either of the following:

(1) Subjecting the employee to discipline or discharge on account of the exercise by the employee of privacy rights guaranteed by Section 1 of Article I of the California Constitution, provided the activity does not substantially interfere with the employee's bona fide job performance or working relationship with the employer.

(2) Denying employment to a prospective employee on account of the prospective employee's exercise of privacy rights guaranteed by Section 1 of Article I of the California Constitution.

(b) Damages awarded pursuant to this section may include punitive damages, and reasonable attorney's fees as part of the costs of the action. If the court decides that an action for damages was brought without substantial justification, the court may award costs and reasonable attorney's fees to the employer.

SEC. 4. Section 502 of the Penal Code is amended to read: [[\*\*\*\* Note that this would AMEND current law. \*\*\*\*]]

502. (a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of

individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system which provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network. (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1),
(2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation which does not result in injury, and where the value of the computer services used does not exceed four hundred dollars (\$400), by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation which results in a victim expenditure in an amount greater than five thousand dollars (\$5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars (\$400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (8) of subdivision (c) is punishable as follows:

(A) For a first violation which does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars (\$250).

(B) For any violation which results in a victim expenditure in an amount not greater than five thousand dollars (\$5,000), or for a second or

subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation which results in a victim expenditure in an amount greater than five thousand dollars (\$5,000), by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

[[\*\*\*\* Use of << STRIKETHRU <> and {{ UNDERSCORE }} begins, hereafter. \*\*\*\*]]

(e) (1) In addition to any other civil remedy available, {{ any injured party, including but not limited to }} the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including {{ consequential or incidental damages. In the case of the owner or lessee of the computer, computer system, computer network, computer program, or data, damages may include, but are not limited to,}} any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. << For <> [[\*\*\*\* Yes, that was a struck-thru "For" ending that paragraph. \*\*\*\*]]

{{ (2) Any person who recklessly stores or maintains data in a manner which enables a person to commit acts leading to a felony conviction under this section shall be liable to each injured party for a civil penalty of ten thousand dollars (\$10,000), up to a maximum of fifty thousand dollars (\$50,000). Failure to report a previous violation of this section to a local law enforcement agency pursuant to subdivision (f) may constitute evidence of recklessness }}

{{ (3) For }} the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

#### << (2) <>

{{ (4) }} In any action brought pursuant to this subdivision the court may award reasonable attorney's fees to a prevailing party.

### << (3) <>

{{ (5) }} A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(f) {{ The owner or lessee of any computer, computer system, computer network, computer program, or data shall report to a local law enforcement agency, including the police, sheriff, or district attorney, any known violations of this section involving the owner or lessee's computer, computer system, computer network, computer program, or data. The reports shall be made within 60 days after the violations become known to the owner or lessee. }}

{{ (g) }} This section shall not be construed to preclude the

applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

<< (g) <>

{{ (h) }} Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

<< (h) <>

{{ (i) }} (1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies and computer services, as defined in paragraph (4) of subdivision (b), which are used do not exceed an accumulated total of one hundred dollars (\$100).

<< (i) <>

{{ (j) }} No activity exempted from prosecution under paragraph (2) of subdivision << (h) <> {{ (i) }} which incidentally violates paragraph (2),
(4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

<< (j) <>

{{ (k) }} For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

<< (k) <>

{{ (I) }} In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

SEC. 5. Section 27565 of the Streets and Highways Code is amended to read: [[\*\* NOTE: This is another amendment, with strikethrus and underscores. \*\*]]

27565. (a) The Department of Transportation, in cooperation with the district and all known entities planning to implement a toll facility in this state, shall develop and adopt functional specifications and standards for an automatic vehicle identification system, in compliance with the following objectives:

(1) In order to be detected, the driver shall not be required to reduce speed below the applicable speed for the type of facility being used.

(2) The vehicle owner shall not be required to purchase or install more

than one device to use on all toll facilities, but may be required to have a separate account or financial arrangement for the use of these facilities.

(3) The facility operators shall have the ability to select from different manufacturers and vendors. The specifications and standards shall encourage multiple bidders, and shall not have the effect of limiting the facility operators to choosing a system which is able to be supplied by only one manufacturer or vendor.

(b) {{ The vehicle owner shall have the choice of prepaying tolls, or being billed after using the facility. If the vehicle owner prepays tolls:

(1) The department or any privately owned entity operating a toll facility shall issue an account number to the vehicle owner. The account number shall not be derived from the vehicle owner's name, address, social security number, or driver's license number, or the vehicle's license number, vehicle identification number, or registration.

(2) Once an account has been established and an account number has been given to the vehicle owner, neither the department nor the privately owned facility shall keep any record of the vehicle owner's name, address, social security number, or driver's license number, or the vehicle's license number, vehicle identification number, or registration.

(3) The vehicle owner may make additional prepayments by specifying the account number and furnishing payment. }}

{{ (c) }} Any automatic vehicle identification system purchased or installed after January 1, 1991, shall comply with the specifications and standards adopted pursuant to subdivision (a).

{{ (d) Any automatic vehicle identification system purchased or installed after January 1, 1993, shall comply with the specifications and standards adopted pursuant to subdivisions (a) and (b). }}

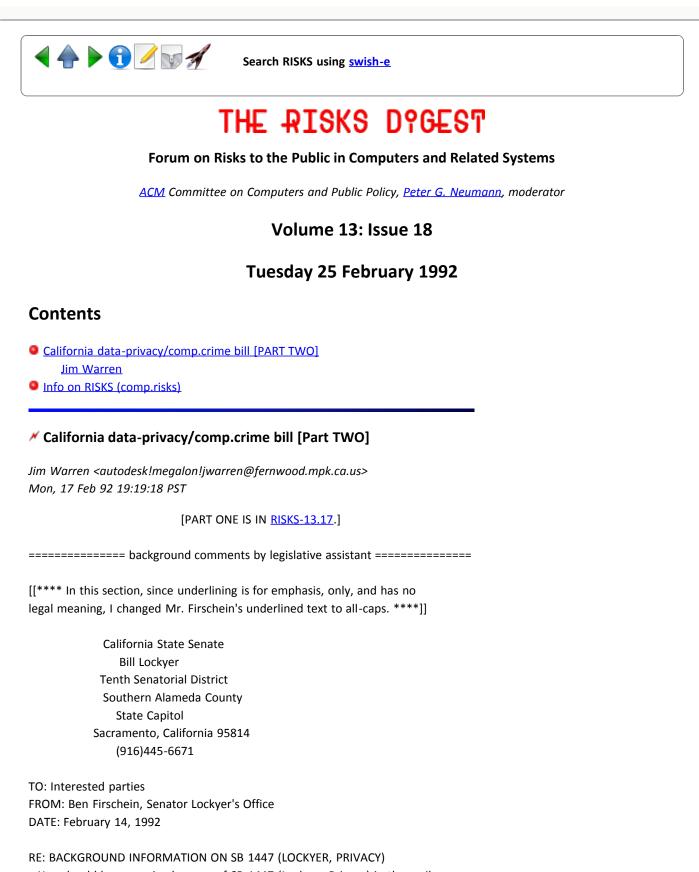
[[\*\*\*\* END OF SB 1447, DATED FEBRUARY 10, 1992 \*\*\*\*]]

[PART TWO IS IN <u>RISKS-13.18</u>.]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



You should have received a copy of SB 1447 (Lockyer, Privacy) in the mail recently. Senator Lockyer introduced the bill in an effort to address some of the concerns raised at the privacy hearing on December 10, 1991.

This memorandum is intended to explain the intent of the various sections of the bill, but it is not a committee analysis.

(A committee analysis will be forthcoming at a later date, when the bill is set for a hearing). We welcome suggestions as to how to clarify the language of the bill, or otherwise improve the bill.

### SECTION 1: CITATION

The bill may be cited as the "Privacy Act of 1992"

### SECTION 2: INFORMATION OBTAINED FROM DRIVER'S LICENSES

This section requires the written consent of a consumer for a business entity to (1) sell information obtained from the consumer's driver's license or (2) use such information to advertise goods or services.

The section is intended to cover instances where a consumer presents a driver's license or identification card for identification purposes during a business transaction. The section is not intended to prevent businesses from using driver's license information for business record-keeping, or for other purposes related to the transaction (i.e. authorizing a transaction).

The section is not intended to change existing law with respect to the ability of businesses to obtain driver's license information from other sources (such as DMV records).

The need for this section is heightened by the new "magstripe" drivers license developed by the Department of Motor Vehicles. This license has a magnetic stripe on the back which contains much of the information on the front of the license. The stripe will enable a business entity to store information contained on a driver's license simply by scanning the card through a reader.

A publication by the Department of Motor Vehicles dated May 1991 ("Department of Motor Vehicles Magnetic Stripe Drivers License/Identification Card") states that "using point of sale (POS) readers and printers, the business community can electronically record the DL [driver's license] /ID number on receipts and business records." The publication notes that "magnetic stripe readers are readily available, relatively low in cost, and are already available in many retail outlets."

However, a merchant might access much more than the driver's license/ID number; the publication notes that "readers have been produced, and market available readers can be modified that will read the three tracks of information contained on the California card." According to the publication, the tracks contain information such as license type, name, address, sex, hair-color, eye-color, height, weight, restrictions, issue date.

### SECTION 3:

### DEPRIVATION OF THE RIGHT TO PRIVACY OF EMPLOYEES OR PROSPECTIVE EMPLOYEES

This section provides that an employer shall be liable to an employee or prospective employee for damages caused by subjecting an employee to discipline or discharge or denying employment to a prospective employee, on account of the exercise by that person of privacy rights guaranteed by the California Constitution.

This section is modeled after Connecticut Labor Code Section 31-51q. The Lockyer bill goes further than the Connecticut statute in that it applies to prospective as well as current employees.

The bill would allow punitive damages and reasonable attorney's fees to be awarded pursuant to Section 3 (page 3 lines 10-12).

The bill would specify that if the court decides that an action for damages was brought by an employee or a prospective employee without "substantial justification," the court may award costs and reasonable attorney's fees to the employer (page 3, lines 12-15).

As with the Connecticut statute, an employee's cause of action would only exist if the activity for which the employee was disciplined or discharged did not "substantially interfere with the employee's bona fide job performance or working relationship with the employer." (Page 3, lines 4-5).

POSSIBLE AMENDMENT: The language in the bill covering prospective employees (page 3, lines 6-9) omits the "substantial interference" language contained in the section covering existing employees. Perhaps the bill should specify that a prospective employee lacks a cause of action if the prospective employer has a compelling business interest in rejecting someone because they engaged in certain acts (even though those acts were protected by the constitutional right to privacy).

Such an amendment would be consistent with cases such SOROKA V. DAYTON HUDSON CORPORATION, 91 Daily Journal D.A.R. 13204 (1st Appellate District). The court in SOROKA found that a psychological screening test administered to Target Store security officer applicants violated the applicants' state constitutional right to privacy when it inquired about their religious beliefs and sexual orientation, because there was no compelling need for the test.

POSSIBLE AMENDMENT # 2: One of the participants in the privacy hearing suggests language making it clear that the rights and remedies set forth in the section are not exclusive and do not pre-empt or limit any other available remedy.

POTENTIAL ARGUMENTS AGAINST THIS SECTION: Some may argue that in light of cases such as Soroka, this statute is unnecessary, because these rights are already set forth in existing case law.

They may also point out that the California Supreme Court held in WHITE V. DAVIS that the right to privacy is self-executing, meaning that every Californian has standing to sue directly under Article I, Section I of the California Constitution for a privacy violation. WHITE V. DAVIS (1975) 13 Cal.3d 757, 775. Given that the right to privacy is self-executing, why is a statute needed?

The answer is that case law is in a state of flux, and there is no guarantee that future courts will construe Article I in such a liberal fashion. Also, the bill is an improvement over existing case law in that it specifically lists the types of damages that may be awarded, including punitive damages, and reasonable attorney's fees.

#### SECTION 4. COMPUTER CRIMES

Jim Warren (one of the witnesses at the hearing) posted the Leg Counsel draft of the bill on one of the networks and showed me some of the responses. This section generated most of the comments, some of which were quite vocal.

First a word of caution to those uninitiated in the ways of the Legislature: MOST OF THE LANGUAGE IN THIS SECTION IS EXISTING LAW. Our proposed additions are contained in language that is in italics or underlined. IF IT IS NOT IN ITALICS OR UNDERLINES, IT IS EXISTING LAW.

PROPOSED ADDITION #1 (page 7, line 25): Extend the existing computer crime statute [Penal Code Section 502] to allow civil recovery by any injured party against someone convicted under Section 502 of breaking into a computer. (The existing law just allows recovery by the owner or lessee of a computer system). For example, if someone is convicted under Section 502 of breaking into TRW's computers and altering credit records, the existing statute would

allow TRW to recover against the hacker in a civil suit, but the statute would not allow someone whose credit history was injured by the hacker to sue the hacker under statute.

PROPOSED ADDITION #2 (page 7, lines 30-33): Extend Penal Code Section 502 to allow civil recovery against a convicted hacker for more than just the cost of expenditures necessary to verify that a computer system was or was not altered, damaged, or deleted by the access. The proposed language would allow civil recovery for ALL CONSEQUENTIAL OR INCIDENTAL DAMAGES resulting from the intrusion.

PROPOSED ADDITION #3 (page 7, lines 38-40 & page 8, lines 1-6): Create a cause of action against those who "recklessly store or maintain data in a manner which enables a person to commit acts leading to a felony conviction under this section."

The section is intended to address the situation where someone stores information (e.g. credit data) in a manner which easily allows unauthorized access, and the person who is able to access the information as a result of the lack of safeguards injures a third party (e.g. a creditor, or a person whose credit history is altered).

The source of the section is the case of PEOPLE V. GENTRY 234 Cal.App.3d 131 (1991). In that case, a hacker figured out that if he queried the credit databases of TRW, CBI, or Trans Union, about a nonexistent person, each system would create a new file for that non-existent person. The non-existent person would have an exemplary credit history, because there was no negative credit information in the new file. The hacker in the GENTRY case went into the business of rehabilitating people's credit history by having them change their name, and then creating credit files on these "new" people.

The court stated in a footnote "we do not address the potential liability to innocent third parties who might be harmed by this feature of the software program. Although Gentry found a weakness in the program and exploited it, responsibility should not rest solely with the felon. Credit reporting companies should recognize that this flaw is needlessly risky and remedy it." (GENTRY, page 135, footnote 3).

POTENTIAL CONCERNS: some people who have seen the bill worry that section 4 would apply to someone (e.g. a computer bulletin board operator) who stores information on a computer about how to commit a crime (e.g. information about how to break into a computer, or how to build a bomb)

The section is intended to be limited to reckless storage of data in a manner which enables a person to commit acts LEADING TO A FELONY CONVICTION UNDER SECTION 503 (not other types of criminal acts). "Reckless storage" is intended to mean maintaining a system that lacks appropriate security safeguards; it is not intended to include storing information about how to commit crimes. Hopefully any potential ambiguities can be clarified through amendments.

PROPOSED ADDITION #4: The bill requires the reporting to local law enforcement of violations of the computer crime statute (Penal Code Section 503) within 60 days after such violations become known to the owner or lessee of a computer system (page 8, lines 26-34). The bill states that "failure to report a previous violation of this section to a local law enforcement agency...may constitute evidence of [reckless storage of data]."

This is intended to ensure that people report such crimes to law enforcement. There are anecdotal reports that some of these crimes are not being reported because people are concerned about bad publicity resulting from reports that their systems were broken into.

POSSIBLE AMENDMENT: it has been suggested that the reporting requirement

be limited to certain types of systems, or to a certain level of monetary loss. Objections have been raised that the bill would apply equally to someone who operates a home computer and to a business that operates a large mainframe. One could argue that the reporting requirement is more essential where a computer owner has a fiduciary or quasi-fiduciary duty to the people whose records are stored on the system (e.g. accounting or credit records). An accountant's or a credit company's failure to report a computer break-in is more serious than a computer game bulletin board operator's failure to report a break in.

One possible objection to restricting the reporting requirement to a certain level of financial loss is that financial loss is hard to quantify.

However, Section 503 already uses amount of financial loss to determine the type of criminal penalty to apply, so one could argue that amount of monetary loss could similarly be used as an indication of the need to report.

### SECTION 5. AUTOMATIC VEHICLE IDENTIFICATION SYSTEMS

Existing law directs Caltrans to develop specifications for automatic vehicle tracking systems for toll facilities, such as those on bridges (Streets and Highways Code 27565). People will soon be able have a device installed in their car which allows them to drive through a toll facility without stopping. The device will send a signal to a computer, which will keep track of their use of the facility. At the end of the month, they will get a bill. Presumably there will continue to be booths that people can drive through and pay cash.

At the December 10 privacy hearing, concern was expressed that the device offers potential for abuse. For example, if you know a particular vehicle is driving through the facility, why not program the system to:

1. Stop all people with outstanding warrants

2. Stop all people who have not paid their vehicle registration

3. Compile lists of all people who drove through the facility during a given month and sell the lists to the private sector.

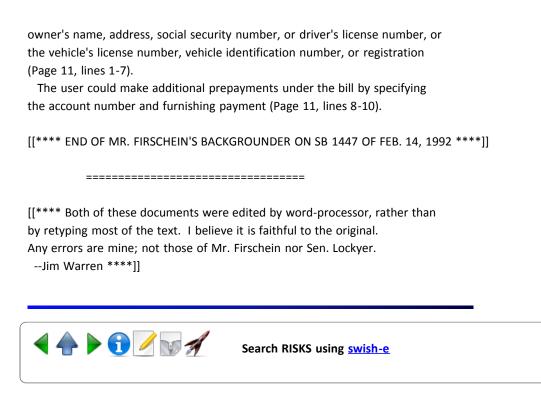
One could argue that uses 1 and 2 are legitimate uses of this technology, because people who have broken the law should expect to come into contact with the police when they drive on public roads and highways. But one could also argue that people have an expectation of privacy when they drive and are not breaking the law at the time they are stopped (e.g. they are not speeding, driving under the influence, or otherwise doing anything to attract the attention of the police).

Use # 3 is harder to justify. Why should people have to reveal their personal lives to the private sector in order to use a device that will speed up their commute?

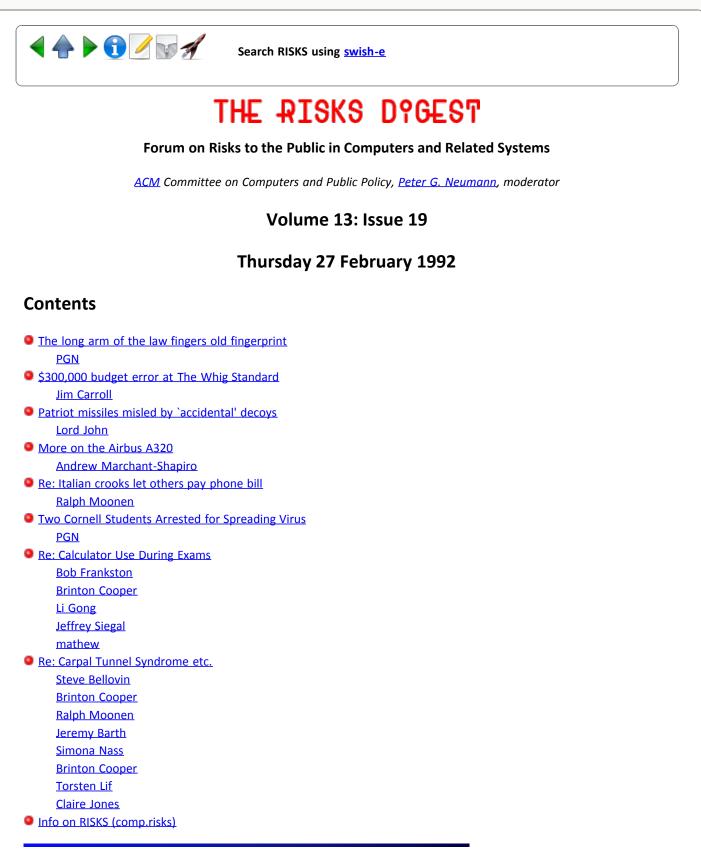
WHAT THE BILL DOES: The bill allows people the option of prepaying their tolls, and then using the facility anonymously. People would continue to have the option of being billed, rather than prepaying tolls.

Under the bill, people who prepaid their tolls would be given an identification number unrelated to the vehicle owner's name, address, social security number, or driver's license number, or the vehicle's license number, vehicle identification number, or registration (page 10, lines 34-40). When they drive through the facility, the facility would look at their account, and let them through if there was still money in the account.

The bill provides that once a numbered account has been established, neither Caltrans nor a private facility shall keep any record of the vehicle



Report problems with the web pages to the maintainer



# M The long arm of the law fingers old fingerprint

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 27 Feb 92 14:51:23 PST A fingerprint found in an unsolved 1984 murder of an 84-year-old woman was kept in the San Francisco police database all these years. Recently the SF print database was linked with the Alameda County database. The old print matched a new one taken in connection with a petty theft case, and so eight years later the police were able to solve the old case (burglary, arson, homicide). The two girls implicated were 12 and 15 at the time. [Source: Article by Stephen Schwartz, Chronicle Staff Writer, San Francisco Chronicle, 22 Feb 1992, p.A16]

### \$300,000 budget error at The Whig Standard

"Jim Carroll" <jcarroll@jacc.uucp> Thu, 27 Feb 1992 09:00:16 -0500

From the Feb. 21 Toronto Globe and Mail...

"A misplaced computer byte has forced a daily newspaper in Kingston to chew a sizeable hunk out of its budget for 1992. The \$300,000 glitch, discovered last month, means the Whig Standard will be hiring only two students to work as reporters or editors this summer instead of five, and also has forced it to reduce its spending for freelance stories, editor Neil Reynolds says. The computer in the newspapers accounting department somehow managed to understate editorial cost by \$300,000 when it spewed out editorial budget planning numbers last fall..... The newspaper is thoght to have a total editorial budget of about \$3 million a year."

What is interesting about this particular error is the size of the error compared to the budget : 10%. Surely some cursory review should have identified an error of this magnitude.

Jim Carroll, J.A. Carroll Consulting, Mississauga, Canada jcarroll@jacc.uucp Voice/Fax +1.416.274.5605 MCI, Bix JCarroll

## Patriot missiles misled by `accidental' decoys

"UKAV03::W0400" <W0400%UKAV03.decnet@usav01.glaxo.com> 27 Feb 92 13:01:00 EST

Quotes from an article in the New Scientist 15 Feb 1992:

The US Army's Patriot missiles missed many of the Iraqi missiles that the US thought they had shot down during the Gulf War, according to a new analysis. Iraqi's modified Scud missile, called the Al-Husayn, was difficult to hit because it was so unstable that it broke into pieces when it reentered the atmosphere, creating a confusing barrage of debris.

Ted Postol, a professor at MIT, re-examined the Patriot's war record at the request of a Congressional committee. He found that deploying Patriot missiles defences did not reduce damage during Iraq's missile attacks on Israel and Saudi Arabia.

Postol then examined videotapes recored by TV journalists that seemed to show

the Patriot missiles successfully intercepting Al-Husayn missiles. Paytheon, the Patriot's manufacturer, has used this footage to promote its missile. Incoming Iraqi missiles are visible on the videotapes because of their velocity, about two metres per second, {that must be a mistype in the article, I expect it should be two kilometers per second W.} makes them glow incandescently as they re-enter the athmosphere. The videotape also captures the explosions of the Patriot interceptors.

Postol played these videotapes in slow motion to an audience of the AAAS. As the Patriot detonations flashed on the screen, Postol stopped the tape to show how far these explosions were from the glowing Al-Husayn warheads. In most cases, the Iraqi Al-Husayn warhead appeared to fly straight on unharmed. In one case, there was a fireball as the Iraqi warhead exploded on impact with the ground.

The army claims that the Patriots successfully intercepted 45 of the 47 missiles they tried to shoot down. But Postol says the tapes show that in some of these cases, the Patriots missed their targets by at least a kilometer. Postal measures this distance by comparing the relative motions of the Patriot fireball, which stays in one place, and the Al-Husayn warhead.

The Patriot had a particularly hard time hitting the Al-Husayn because of problems with the Iraqi missile. Iraqi engineers had extended the range of the Soviet Scud-B missile by lengthening its fuel tanks and making its warhead much lighter. The changes made the missile unstable, and caused the Al-Husayn to flop belly-first as it re-entered the athmosphere, often breaking up in the process. the Patriot missile had to distinguish between the Al-Husayn's warhead and other debris such as the empty fuel tank and tail fins which rained from from the sky. In effect, the Iraqi missile released unintended but effective "decoys" to distract the Patriot, said Postol. Ther Patriot had its own problems as well. One software bug could have directed the Patriot to attempt to intercept an incoming missile at a point below ground. In one case this bug may have caused a Patriot to turn back and dive into the ground.

Postol argues that the effectiveness of the Al-Husayn's unintended decoys shows how extremely simple factors can frustrate attempts to shoot down ballistics missiles. This could teach scepticism when it comes to evaluating the claims made for missile defence technologies, such as plans for the US Star Wars system.

Raytheon disputes Postol's conclusions, but has not yet made public a detailed analysis that would rebut his claims. Defenders of the Patriot believe the damage on the ground could have come from falling debris rather than from detonations of the Iraqi missile's warhead.

[It is funny how what starts as a great success, turns out less than so, when investigated. It also demonstrates that very simple systems can (and do) prevent the high technology systems working, as well as showing that designers of such systems get a mindset as assumes the opponents have the same mindset. This is not always so... Lord John - The Programming Peer]

### More on the Airbus A320

"MARCHANT-SHAPIRO, ANDREW" <marchana@gar.union.edu> 25 Feb 92 13:55:00 EDT

On National Public Radio's Morning Edition program this AM, one report concerned the series of crashes that have plagued the Airbus 320. According to this report, MOST 320 aircraft have an alarm that informs the pilot that s/he is flying too low, but France does not require this alarm and so aircraft sold to and/or operated by French companies do not have this alarm installed.

I don't even qualify as a dabbler in this area, but if I recall correctly, at least 2 out of 3 crashes, and possibly all 3, involved French aircraft. Since they have also been somewhat similar (an apparently \_unnoticed\_ loss of altitude), could this help to explain what happened?

If so, this points to a particularly interesting human interface problem -perhaps the A320 tends to drop faster than other aircraft, but, since there is no alarm, [some] pilots do not realize what is happening until they're too low to do anything about it.

Any comments from qualified persons?

Andrew Marchant-Shapiro, Depts of Sociology and Political Science, Union College, Schenectady NY 12308 518-370-6225 marchana@union.bitnet

## Ke: Italian crooks let others pay phone bill (Weber, <u>RISKS-13.16</u>)

<rmoonen@hvlpa.att.com> Tue, 25 Feb 92 11:14 MET

There was a big case in the Netherlands over 5 years ago where they did the same. The scheme involved renting a mobile phone from the Dutch PTT, copying the EPROM, transfering the EPROM to a mobile phone which had been stolen, and then returning the rented phone. This way, as the phone gets re-rented again to various persons, the bill gets spread out, and it will be less obvious.

BTW, what inferior kind of ATM's do they have in Italy that let you tamper with the EPROMS inside? Maybe we have some over here in Holland too? :-)

# Two Cornell Students Arrested for Spreading Virus

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 25 Feb 92 13:12:23 PST

2 Cornell Students Arrested for Spreading Computer Virus LEE A. DANIELS, N.Y. Times News Service

Two Cornell University undergraduates were arrested Monday night and charged with developing and spreading a computer virus that disrupted computers as far away as California and Japan, Cornell officials said. M. Stewart Lynn, vice president for information technologies at the university in Ithaca, N.Y., identified the students as David Blumenthal and Mark Pilgrim. Lynn said that both Blumenthal, who is in the engineering program, and Pilgrim, in the college of arts and sciences, were 19-year-old sophomores. They were arrested Monday night by Cornell and Ithaca police officers. Lynn said the students were arraigned in Ithaca City Court on charges of second-degree computer tampering, a misdemeanor, and taken to the county jail. Lynn said authorities believed that the two were responsible for a computer virus planted in three Macintosh games on Feb. 14. [...]

He identified the games as Obnoxious Tetris, Tetricycle and Ten Tile Puzzle. The virus may have first appeared in a Stanford University public computer archive and spread from there through computer users who loaded the games into their own computers.

Lynn said officials at Cornell and elsewhere became aware of the virus last week and quickly developed what he described as ``disinfectant'' software to eradicate it. He said officials traced the virus to Cornell last week, but he would not specify how that was done or what led officials to the two students. Lynn said he did not yet know how much damage the virus had caused. ``At Cornell we absolutely deplore this kind of behavior,'' he said.

[reference to RTM deleted.]

AP item notes both are being held in the Tompkins County Jail on \$10,000 bail.

# Ke: Proposal for policy on calculator use during exams (Bezenek 13.16)

## <Bob\_Frankston@frankston.std.com> Tue 25 Feb 1992 20:14 -0500

The long term issues are challenging. In a very few years, the subtablet-size portable computer will have replaced the calculator as the issue for exams. These systems will have a few megabytes (32, 64, 1GB?) of space (between the paging devices and the primary memory) and a full GUI interface. They will be preferable to notepaper (especially the pen or its successors complementing the keyboard). Even more so than the current personal computers, these systems will be an integral part of how people solve problems. Since they are also the reference devices, it is unclear what the distinction will be between and open book exam and a closed book (def: a device for presenting information) exam.

Of course, one can ban them from closed book exams, but that would reduce closed book exams to an abstract exercise unrelated to actual practice.

The problems become worse when we have the WAN infrastructure so that the systems have builtin packet radio connections that are an integral part of their operation. While we can still have Faraday Cage exams, they too would be useful for testing the ability to survive without intellectual assists, but would not test the more important ability to take full advantage of the technologic infrastructure.

While I sometimes go off the technical deepend in predicting what is going to happen, I'm already working with the early forms of these technologies so the issue is one of timing rather than possibility.

Considering that computers have still had little impact on the educational system, once these systems drop below crucial price points they will rapidly overwhelm the schools. I'm presuming the appropriate UI's will be available and that the impediments are mainly economic.

## Ke: Proposal for policy on calculator use during exams (Bezenek 13.16)

Brinton Cooper <abc@BRL.MIL> Tue, 25 Feb 92 9:12:19 EST

Todd M. Bezenek KOON <plains!bezenek@uunet.uu.net> communicates his proposed policy regarding the use of calculators on closed note university exams. In brief, he would take possession of a device which he (the proctor) believes to have been used to violate the intent of closed-note examinations. He would have a faculty member judge whether the calculating machine and its memory content provided an illegal aid to the test-taking student.

I guess he never heard of "due process." If you try that in universities supported by public funds, you run the risk of being sued by the student. His procedure sets up a couple of faculty as a "kangaroo court" (what does that mean, anyhow?) to judge whether a student cheated.

High-tech times may call for low-tech solutions. I simply do not permit the use of calculating devices on Computer Science examinations and quizzes. The reasoning is simple:

Programmers should be proficient, personally, in computation.

- a. Having to work out a few numerical examples by hand can help budding programmers hone their ability to see more than one way to do a computation.
- b. Using this ability can provide "sanity checks" on their software.
- c. Programmers should be able to get the answer even when their batteries have run down.

I fear that at least some of the human-induced software faults discussed so often in this forum can be traced to the lack of computational skill on the part of the programmer involved.

\_Brinton Cooper abc@brl.mil cooper@udel.edu ab.cooper@compmail.com

#### Ke: Proposal for policy on calculator use during exams (Bezenek 13.16)

Li Gong <li@cambridge.oracorp.com> Wed, 26 Feb 92 14:47:31 EST

In <u>RISKS-13.16</u> Todd M. Bezenek proposed a policy for dealing with "the use of calculators on university exams." His posting "demonstrates the risk of introducing computing power into the classroom where it may be misused."

Unfortunately, such a policy, short of banning a student from using his/her \*own\* calculator, could not beat technology. For example, it is easy to imagine a calculator that can be activated only by a (say 10 digit) PIN. Today's photocopiers can operate in this fashion. The new trick is to require periodical input (say every 3 minute) of the PIN. If PIN is not typed in in time, the calculator locks itself, and starts scrambling some parts of the memory (using the PIN as key). then erase the key from memory afterwards. To find any evidence of wrong doings, the memory section in question has to be examined within 3 minutes.

The basic point is that if a student has his/her own Trusted Computing Base, no one can beat him/her. If this is not true, nobody would work in the field of computer security today. So ban the calculators, or supply "official" ones during exams.

Li Gong, ORA Corp, 675 Mass Ave, Cambridge, MA, USA.

#### Ke: Proposal for policy on calculator use during exams (Bezenek 13.16)

<jbs@congruent.com> Tue, 25 Feb 92 11:16:44 EST

You might want to consider portable computing devices with wireless communications capabilities (packet, cellular, etc.)!

Jeffrey Siegal

#### Ke: Proposal for policy on calculator use during exams (Bezenek 13.16)

From A to B <mathew@mantis.co.uk> Wed, 26 Feb 92 17:25:43 GMT

At the risk of starting a lengthy and somewhat off-topic debate, I'd like to remark that I don't think there's actually any technological risk involved here.

The "problem" is that calculators with memories enable students to store data and retrieve it during the exam. The only reason this is a "problem" at all is that almost all exams are based around parrot-style repetition of memorized "facts".

The solution to the "problem" is to allow all students to take in whatever reference materials they like. Then the examination will necessarily have to be a real test of problem-solving ability rather than a test of the candidate's ability to regurgitate memorized data.

Of course, the problem then is that ability in examinations might in some way tally with the candidate's ability to work in real-world situations.

> The calculating device shall remain in the possession of the

> proctor until the contents of its memory--both vendor supplied and user > programmed--can be examined.

What exactly are you going to do about the "vendor-supplied" part of the memory? Many calculators now have common physical constants stored in their ROMs; is that unfair to those who aren't allowed to take in a databook?

If so, doesn't that mean that allowing people to take in a calculator which performs logarithms or statistical functions is unfair to those not allowed to take in log tables or statistical analysis reference books? mathew

#### Ke: Carpal Syndrome reports rise sharply (Cooper)

<smb@ulysses.att.com> Mon, 24 Feb 92 20:32:00 EST

Brint Cooper states that all sufferers from carpal tunnel syndrome that he knows are cashiers, and that none of the computer folks he knows suffer from it. He goes on to wonder if stress may play a role. I can't answer that question, but I can state, from both first-hand and second-hand knowledge, that computer users do indeed suffer from carpal tunnel syndrome.

In my own case, the carpal tunnel syndrome is fairly mild -- but I have bad problems with tendonitis. Nor was the orthopedist in any doubt about what caused my symptoms -- his first question to me was ``do you use a computer keyboard much?'' He went on to state that most of his patients with tendonitis of the wrist or elbow, or carpal tunnel syndrome, were heavy computer users.

That aside, I also know of several others who have suffered from both problems, including at least one who needed surgery. Psychological stress may contribute -- but don't discount the purely-mechanical.

--Steve Bellovin

#### Ke: Carpal Syndrome reports rise sharply

Brinton Cooper <abc@BRL.MIL> Tue, 25 Feb 92 0:24:28 EST

No, I don't discount the physical causes of carpal syndrome, tendonitis, and other occupational risks of keyboards. But I must tell you of my daughter who had such a case of tendonitis at age 14 that her hand literally locked up at the (piano) keyboard during a music lesson. I don't believe I'm violating her privacy to relate that this was a very stressful time for her for many reasons. Today, 15 years later, she's got a handle on the stress. Also, she can and does play piano for 5-6 hours at a time. It's necessary; it's how she makes her living.

Physicians and others who are looking for the connection between computer keyboards and orthopaedic disease must consider the stress factors. I'd HATE to spend 8-9 hours per day keyboarding credit card information for VISA, but

I've often spent that much time and more at keyboards building software, doing computations, and writing scientific reports. If we're going to build a low-risk workplace, we must address \*all\* the risks, not merely those that are fashionable.

\_Brint

#### ✓ Carpal Syndrome (Cooper)

<rmoonen@hvlpa.att.com> Tue, 25 Feb 92 11:14 MET

I know several sufferers of CTS, and all of them are musicians. My mother was operated on both wrists, and she never had any problems with it any more. Likewise with the other musicians I know. (Most notedly string players) Here at wotk also I know of at least one case, in which the sufferer was a programmer. So also keyboard action can give it you for sure. I am pretty sure that stress and other psychological factors are involved, but bad muscular techniques are the no. 1 cause.

--Ralph Moonen

# ✓ Carpal Syndrome: Is it just psychosomatic? (Cooper)

Jeremy Barth <pubmail!barth@uu2.psi.com> Tue, 25 Feb 92 10:34:25 EST

I detect a dangerous elitism in this kind of observation. The author makes a sociological generalization based upon a tiny, non-random observational sample with no controls. We all tend to do this, but let's recognize that it's sloppy thinking.

Just two points (the first about the social categories affected, the second about cultural anthropology):

1. The syndrome occurs in all kinds of work environments. In my own personal sphere, which again is non-representative, two of my friends suffer from the syndrome. They're Associated Press reporters in a fancy, white-collar New York office who work on outmoded, non-ergonomic keyboards that are holdovers from AP's early computerization efforts. There's a potentially precedent-setting class action suit wending its way through the courts involving numerous AP reporters who report the syndrome. There are people in their early 30's who can't do simple things without pain, like raising a full cup of coffee to their lips.

2. If you've studied anthropology, you know how hard it is to "see your own kind." All social theorizing has built into it lots of preconceptions we're only minimally aware of. Brinton says he's not aware of reports among his colleagues of CT syndrome; having worked for 2 years in a fast-paced immunology research lab, I would suggest that many hard-driven people choose to ignore substantial pain in pursuit of their goals. (Ever heard about the football player who had his pinkie cut off, rather than submit to a lengthy course of surgery, so he wouldn't have to miss 4 weeks of the season?)

Jeremy Barth

# Kisks of making judgments about job satisfaction (Helegesen)

Simona Nass <simona@panix.com> Tue, 25 Feb 1992 19:34:31 GMT

Do harp players have low job satisfaction? Are they doing it only for the money? It's probably inaccurate to say that all cashiers/secretaries/etc. are unhappy in their jobs. While these exceptions may not entirely refute your anecdotal evidence, I think a better causal explanation can be found. Even if most people getting CTS are not satisfied with their jobs, you need something that explains why those who are satisfied also develop it. Something involving the type of repetitive movement is probably a more proximate cause of the injury.

I wonder if the low incidence of CTS among your computer lab friends is explained by the way they type? Do most programmers touch-type using all ten fingers? Also, how fast do they really type, anyway? I type between 50 and 90, depending on the keyboard. Someone can manage to type fairly quickly (tho' not 90 wpm) using a few fingers, but the TYPE of repetitive movement is different. Also, most computer programmers can't type as quickly when they actually have to compose what they are typing. Some of their time is also spent searching, scanning the text, compiling, munching M&Ms <tm> ... :) -S. -- Disclaimer: I am not an attorney, though I do have an opinion on everything.

( simona@panix.com or {apple,cmcl2}!panix!simona )

#### 🗡 Carpal Risks

Brinton Cooper <abc@BRL.MIL> Tue, 25 Feb 92 16:25:58 EST

I didn't expect the reaction that my piece on the relative risks of the physical act of repetitive keyboarding and of the psychological pressure under which many keyboard users must work. Clearly, the risks attributable purely to repetitive keyboarding, improper terminal and chair adjustments, lack of breaks, poor lighting, etc overwhelmingly dominate the issue.

While I remain committed to being alert to the effects of stress, I yield to the many thoughtful people who wrote to me and spoke, often sadly, of colleagues and associates who live with chronic pain directly attributable to such work. A few have even been ruled permanently disabled. This is worse than unfortunate, and I fear I misguided myself on the issue. \_\_Brint

#### Ke: Carpal Syndrome reports rise sharply (Cooper)

<Torsten.Lif@eos.ericsson.se> Wed, 26 Feb 92 08:52:16 +0100 Let me then point out another major group of CTS sufferers who are (at least) as highly motivated as any hacker: Cyclists. Especially the ones who also do a lot of keyboard work, but even some who do no keyboard/computer work have been afflicted.

#### [...]

Having worked in a similar environment without any ill effects, I was more than dismayed when I started showing the classical symptoms of repetitive motion syndromes after I transferred to computer support. A period of very informal empirical studies (I experimented :-), indicated that the culprit was the type of work, not the system hardware. In essence: Using my SUN workstation as a word processor to enter large amounts of text (on subjects I find interesting and stimulating) is very prone to give me various pains and numbness symptoms in neck, shoulders, arms and hands. Using the same workstation to edit and debug programs is much less fatiguing. I can easily do programming work for a full workday without problems. Just a couple of hours of word processing is enough to give me back all the problems.

I started looking at how I work in these two situations and came to the conclusion that the difference is quite large. Entering text I type for long unbroken periods, moving my arms very little. Editing source code (even when entering it the first time), I move about much more. I use the mouse and/or cursor keys to go back and correct an indentation; I copy a chunk of code I'm too lazy to write again; I look at the debugger, resting my chin in my hand while I try to figure what's wrong; I click the "Step" button and stare in disbelief as the program takes the wrong branch in a "switch"; I scratch my head and take a sip of tea. In other words, programming work is much less (physically) monotonous.

- |> What part does psychological or emotional stress play in the
- |> development of repetitive-motion disorders?

It wouldn't surprise me if the presence of stress hormones in the body aggreviates the problems but my belief is that the nature of the work is much more important. And it is possible that I like programming better than documenting (who doesn't? :-) to the extent where this causes part of the difference for me. But I don't think this accounts for all of it. If it did, why would writing articles for UseNet cause similar pains?

Torsten Lif, Ericsson Telecom AB, EO/ETX/TX/ZD, S-126 25 STOCKHOLM, SWEDEN Phone: +46 8 719 4881

#### // (More on) Carpal Syndrome (Cooper)

<ccmj@dcs.edinburgh.ac.uk> Wed, 26 Feb 92 15:00:16 GMT

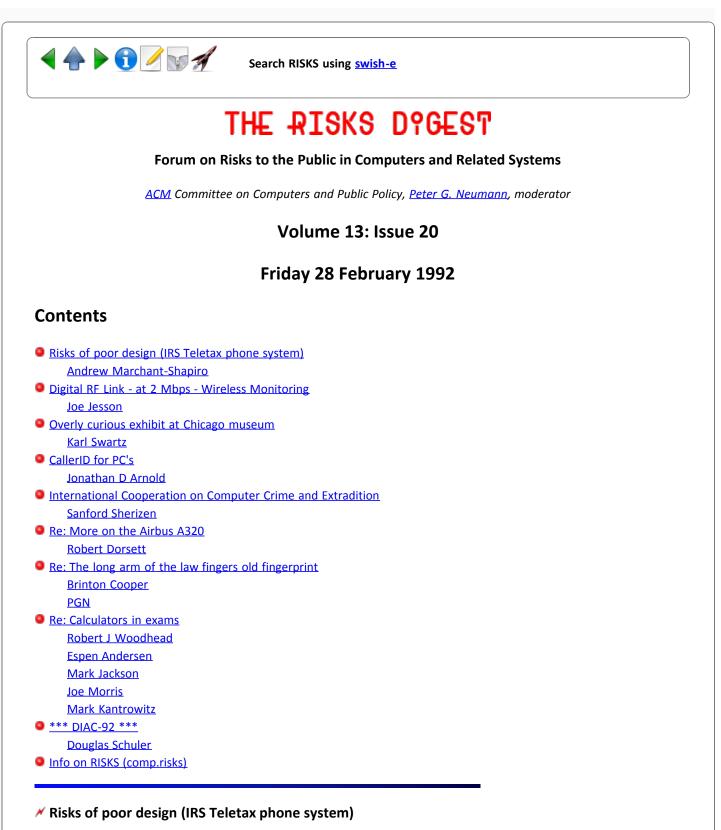
I disagree with the theory. I spend a lot of time \*sitting\* at a keyboard and so do many others here. But we don't spend a lot of time bashing keys with our fingers because we frequently stop to think. I'm sure other computing labs are the same. People like us don't come anywhere near the kind of keystrokes an hour achieved by people doing repetitive keyboarding jobs like copy-typists, data entry clerks etc. If a job requires some tedious keyboarding, we typically have the freedom, knowledge and hardware required to automate it. Mostly people here complain about eyestrain and backache, not carpal tunnel syndrome.

I would also caution Mr Cooper that his theory is liable to misinterpretation by those who would like to dismiss such injuries as malingering by people who want to get out of boring jobs. -- Claire Jones ccmj@dcs.ed.ac.uk



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# "MARCHANT-SHAPIRO, ANDREW" <marchana@gar.union.edu>

27 Feb 92 19:35:00 EDT

Earlier this evening, I tried to find out the status of my refund from the IRS. I called up Teletax, the IRS's voice-mail-like system, and followed the instructions. In general, these seem to be well-done; the most-requested functions are first on each menu, and things seem to be done consistently. I say "seem" for a very good reason...

Following the instructions, I entered my SSN, heard it repeat back, and confirmed that it was correct. I was then told to enter my filing status, which I was about to do, when I heard "error, error, I cannot process your request!" repeated several times. Thinking that the system had burped, I hung up and dialed again. Once more, I gave the machine my SSN. But now, I was given a message to the effect that the IRS updates the system approximately every seven days, that my status had not changed since my last call, and that I should wait seven days before calling again. And, oh yes, thanks for using Teletax.

Now, I know that I probably shouldn't complain about this, since the whole thing is a freebie, but it is truly irritating. A well-designed system would (I think) have told me SOMETHING about the nature of the error, rather than sounding like it dropped out of Lost in Space (come to think of it, THAT robot was a good deal more informative than Teletax). What bothers me most about the system is its assumption that, once the SSN is entered, you have a completed transaction. I haven't tested this out yet, but I'm willing to bet that entering a bogus number (which, btw, gets you a 'your return has not yet been processed') a second time would get you the same message that I got -- call back in seven days.

Of course, this is a minor risk -- it's really more a case of poor error-handling. If I were a true paranoid, I guess I could see some legal claim based on the notion that computer records show me having been apprised of something when I was not; but for now, it's just an irritation. The only real RISK is that someone who enters somebody else's SSN by mistake would, while not getting the other person's information, effectively block the correct person from their information for approximately seven days. [...]

Andrew Marchant-Shapiro, Depts of Sociology and Political Science, Union College, Schenectady NY 12308 518-370-6225 marchana@union.bitnet

# ✓ Digital RF Link - at 2 Mbps - Wireless Monitoring

## Joe Jesson <jessonj@nic.cerf.net> 28 Feb 92 03:09:30 GMT

With all the recent interest in wireless communications, I was somewhat surprised at a recent NCR meeting. On display was an NCR WaveLAN wireless network card. No big deal, I thought, since wireless Local Area Network cards are produced by several companies using different wireless media. Radio Frequency and infrared seem to be the wireless media of choice with one limiting aspect - coverage of one room or, at most, a single office floor.

Since the WaveLAN product uses 902 - 928 MHz no-license band, I assumed the one floor 100 foot limitation.

Here is the surprise; a FIVE MILE distance between transmitter-receiver!! At 2 Mbps!! Real DX for a 250 Mw Digital System... I asked the NCR salesman to confirm this unusual claim. He said a "typical" distance in an enclosed office is 100 - 800 feet but, with an optional antenna and direct line-of-sight path, five miles IS reasonable. He did not have info on the optional antenna. I would assume, at 902 Mhz, the size of the antenna has to be small (even a directional multi-element yagi at 902 Mhz is really small). Ethernet (CSMA/CA) protocol with a low RF bit error rate of 10 exp -8 (at 5 miles?).

Using spread spectrum and optional DES encryption, the 2 Mbps could represent a T-1 data stream with some overhead bits (2 - 1.544 Mbps) potentially as a Local Loop replacement or a no license repeater system. Since the antennas are directional and spread spectrum would allow simultaneous transmissions over the same frequency band (with an increase in noise level). INTERESTING applications and security aspects for a wireless 2 Mbps, 250 Mw power, Spread Spectrum , Differential Quadrature Phase Shift Keying Modulation (DQPSK) system...

Joseph E. Jesson, 21414 W. Honey Lane, Lake Villa, IL, 60046 (day) 312-856-3645 (eve) 708-356-6817; jej@chinet.chi.il.us mhs!amoco!joseph\_e\_jesson@attmail.com [FORGET ATTMAIL UNTIL THEY GET THEIR ACT TOGETHER. THEY HAVE BEEN KILLING ME WITH RAMPANT BARFMAIL. This is an editorial comment based on a month of agony. PGN]

#### ✓ overly curious exhibit at Chicago museum

Karl Swartz <kls@ditka.chicago.com> Thu, 27 Feb 92 2:28:10 PST

I was back home in Chicago several weeks ago and visited the Museum of Science and Industry one afternoon. The Post Office sponsored an area with exhibits on how our mail gets (mis)delivered. One of these was a computer which would tell you your 9-digit zip code, based on a normal address screen:

NAME APARTMENT NUMBER STREET AND NUMBER CITY AND STATE 5-DIGIT ZIP CODE

I recently moved and was mildly interested so I gave it a try with my old (as a check) and new addresses. But right of the top it occurred to me ... why do they need my name?! They don't, but I'm sure many folks just blindly type it in. If this data were actually accumulated by the exhibit (I have no reason to believe it is) one could envision all sorts of potential uses and abuses.

(I believe the thing got testy if one left the name blank; I used the "dummy" name Dan Quayle. :-) )

Karl Swartz, 2144 Sand Hill Rd., Menlo Park CA 94025

#### 1-415/854-3409 UUCP uunet!decwrl!ditka!kls

[GOOD FOR YOU! Now just wait for the mailing lists... PGN]

#### Ke: overly curious exhibit at Chicago museum (responding to PGN)

Karl Swartz <kls@ditka.chicago.com> Fri, 28 Feb 92 3:02:13 PST

<prin> I thought that might catch someone's attention! But I'm not sure they could get the mail to me -- I recall something a few years ago where somebody sent a letter to Ronald Reagan in (wherever), CA. It came back stamped "moved, forwarding address unknown".

Of course I shouldn't pick on government workers too much since as a SLAC employee I'm one of 'em.

#### CallerID for PC's

Jonathan D Arnold <jdarnold@world.std.com> Wed, 26 Feb 92 17:28:43 -0500

New for PC: \$79 Caller ID Device 02/17/92

ROSWELL, GEORGIA, U.S.A., 1992 FEB 17 -- A start-up company announced a device which lets your PC access callers' numbers using the Caller ID service, at a price of \$79. Whozz Calling? is a box, a few inches square, which connects to the phone line using standard RJ-11 jacks and to an IBM-compatible PC through a 9-pin RS-232C port.

Zeus Phonestuff President Mark Sutherland says the device is designed for applications like inbound call management, mail list creation, and modem security. When linked to an online system, for instance, the device can assure that only calls from designated numbers get through. Software comes bundled with it.

"We intend to go into mail order to see what markets are interested in the device, then go to distributors. They need a track record before they pick it up," he said.

Caller ID is becoming available in increasing numbers of states, usually with a provision that callers be able to block their numbers from going out, free, on a per-call basis. The Federal Communications Commission has suggested per-call blocking might become a national policy but a number of states, including Georgia, do not allow consumers to block the sending of the number.

Press Contact: Mark Sutherland, Zeus Phonstuff, 404-587-1541

[This announcement was found on RelayNet, an IBM PC store and forward network.]

Jonathan Arnold, BBS Phone: (617)335-6842 Home Phone: (617)335-5457 Internet: jdarnold@world.std.com uucp: uunet!world!jdarnold

# International Cooperation on Fighting Computer Crime and

Sanford Sherizen <0003965782@mcimail.com> Fri, 21 Feb 92 16:51 GMT

Extradition of Computer Criminals Re: Police Foil Million Pound Hacking Plot (Bob Frankston, PGN)

Bob Frankston and PGN raise some interesting questions about extradition problems with the recent UK hacking plot. However, that particular case does not prove that extradition is impossible. Work on improving international cooperation in fighting computer crime, including extradition of computer criminals, is developing on the political agreements and cross-border law enforcement levels.

Several years ago, I developed a project on how crime control problems have become an important aspect of foreign policy and international agreements. A few of the more active areas of this trend are fighting drug smuggling, anti-terrorist coordination, stock market regulation, and riot control/civil unrest training.

Slowly, computer crime has become part of this international agenda. Many of the international efforts that affect computer crime are related more to financial fraud and money laundering efforts. While these efforts may not explicitly mention computer crime, some attention has been paid to the fact that much of financial fraud and money laundering today is computer-aided. In essence, computer crime is covered by many of these "other" crime control efforts.

Here are some specific examples of this international cooperation.

The European Commission has developed a number of directives and regulations that relate to computer crime issues in the Single Market Europe. The most directly related are the various information protection, privacy, copyright and computer evidence requirements. Some of these have been adopted from the Council of Europe while other are derived from various EC actions. Computer crime-related decisions are also found in EC decisions regarding banking, EDI, and other important industry/sector areas. If anyone is interested in details on the security aspects of EC '92, they can contact me for my recent article in \_Computers and Security\_, which is adapted from my book published by Lafferty Publications in Dublin in 1990.

International law experts have also been been attempting harmonization of law. Extradition has been considered. Recognition has been given to a requirement that offenses shall be punishable under the laws of both the requesting and the requested country and that the offense in question must be of sufficient seriousness. Conventions concerning mutual assistance and extradition have been discussed at the Council of Europe Select Committee of Experts level and the UN has created the UNCITRAL, which relates to aspects of the problem. ITSEC may also create opportunities for classified discussions of these problems.

The BCCI case will probably make this international cooperation even more solid. Even before this case, significant international cooperation had developed regarding the fight against money laundering. Banks are increasingly being forced to give information about depositors to their governments and to act as "quasi-investigators" in responding to suspicious deposits. Even the Swiss banking system, known for its secrecy, has changed significantly in recent years in response to highly publicized money laundering cases and international crooks/political figures. Once again, although not explicit in the legal language or the media coverage, computer-aided crime is a major issue in these situations.

As of last year, the U.S. had a number of bilateral agreements between regulations in markets around the world. U.S. pacts have been signed with the EC on regulating world financial marketplace as well as securities industry reviews. An important regional agreement was signed between the U.S. Securities and Exchange Commission and the Inter-American Development Bank, which could affect some of the Asian exchanges that are now becoming active in Latin America. Again, computer crime is not explicitly discussed in these agreements but they are inherent in the nature of the regulations.

The EC has created the Unite de Coordination de la Luttee Anti-Fraude (UCLAF), which seeks to coordinate anti-fraud activites within the EC. I do not know whether there are extradition aspects to this. I got this information from Gary Marx from MIT, who is working with European criminologists on research concerning policing across national borders.

Finally, PGN raises the question of possible data havens, where people will be free to electronically cross borders but be safe from punishment. Adrian R. D. Norman raised that issue many years ago in his book, "Computer Insecurity" in 1983 Worth reading even today.

Sanford Sherizen, Data Security Systems, Natick, Massachusetts, USA

#### Ke: More on the Airbus A320 (Marchant-Shapiro, <u>RISKS-13.19</u>)

Robert Dorsett <rdd@rascal.ics.utexas.edu> Fri, 28 Feb 92 01:59:15 CST

> According to this report, MOST 320 aircraft have an alarm that informs> the pilot that s/he is flying too low, but France does not require this ...

You're referring to a Ground Proximity Warning System (GPWS). Air Inter did not have them, because the A320 was only used within France, and, as you say, French law doesn't require them. The Habsheim crash involved an Air France airplane, which was used in continental operations; it did have one. The Bangalore crash, which involved an Indian Airlines airplane, also had one.

GPWS was mandated in the US following the 1972 crash of an Eastern Airlines L-1011 in the Florida Everglades. The crew was distracted by a minor systems

problem; in the process, the altitude-hold feature of the autopilot was disengaged. The airplane then very slowly started a descent, and ended up flying into the ground. Nobody was minding the shop. Following the US decision to require them, most other countries followed suit.

The GPWS normally works by comparing radio altitude (actual height above ground), speed, and vertical speed rates. Because of the radio altitude component, it's only effective after the airplane has been flying under approximately 2500' for some length of time.

On the A320, there are five distinct modes which are handled by the system, with corresponding aural alerts:

Excessive rate of descent"Sink Rate" and "Whoop! Whoop! Pull Up!"Excessive terrain closure"Terrain Terrain. Whoop! Whoop! Pull Up!"Altitude loss after takeoff"Don't Sink!"Unsafe terrain clearance"Too Low Gear!" and "Too Low Flaps!"Descent beneath glide slope"Glide Slope!"

The aural messages are normally taped, but knowing Airbus, they're probably digitized. :-) A master caution (yellow--not a warning light) also appears. Most airliners have some variation on the above.

The pilot is able to inhibit the various modes, through four smart switches.

Following the introduction of GPWS after the EAL crash, there were numerous false warnings, and GPWS got a bum rep among many pilots. The system still has problems, due to its basic design premise, but the number of false alarms has dropped significantly, overall. Air Inter has stated that it \*removed\* its units because of excessive false warnings, i.e., operational considerations. Which raises the question that, even if the ill-fated A320 HAD the devices, the crew might very well have ignored the alert.

As with most crashes, the Air Inter crash was likely the result of a complex number of factors; no single protection could have "saved" the airplane.

As for Habsheim, the GPWS went off once, during the set-up to the flyover, but after that, the last few seconds of the approach was beneath the threshold arming altitude of 30'. Which was also beneath the trees. It wouldn't have made any difference.

At Bangalore, there were two excessive rates of descent warnings, but the crew either ignored them, didn't hear them (unlikely, since they're quite loud), or filtered them out.

A very basic lesson here is that if we're going to mandate these systems, we'd better make sure their warnings are accurate. To do otherwise is to limit the effect they may have on pilots, who tend to have more confidence in their airmanship than with a poorly functioning subsystem. Similar arguments can be applied to the imperfect T/CAS 2 system, which was mandated following a highly publicised mid-air collision. Too many wrong warnings can be worse than none at all.

Robert Dorsett UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

# \* Re: The long arm of the law fingers old fingerprint

Brinton Cooper <abc@BRL.MIL> Thu, 27 Feb 92 20:07:18 EST

You write of "A fingerprint found in an unsolved 1984 murder" and which fingerprint ... matched a new one taken in connection with a petty theft case..." leading to solution of the murder! This isn't the sort of thing we usually see in Risks Digest. This time, the risk is "good," as it was a risk to the bad guys!

\_Brint

# Re: The long arm of the law fingers old fingerprint

RISKS Forum (Peter G. Neumann) <risks@csl.sri.com> Thu, 27 Feb 92 18:38:22 PST

Brint, You are absolutely correct. I could have added a nice note at the end, soliciting more HAPPY stories. I used to get a lot of grumbles from folks who say we never run anything but the bad news. But we don't get much good news submitted. I had to submit that one myself! Peter

# Re: Calculators (<u>RISKS-13.19</u>)

Robert J Woodhead <trebor@foretune.co.jp> Fri, 28 Feb 1992 03:06:06 GMT

>... Then the examination will necessarily have to be a real test of
> problem-solving ability rather than a test of the candidate's
> ability to regurgitate memorized data.

Alas, this would add the requirement that the teachers be capable of asking good questions. In all but a few cases, this may be too much to ask. ; $^{n}$ )

Robert J. Woodhead, Biar Games / AnimEigo, Incs. trebor@foretune.co.jp

# Re: Calculator Use During Exams

ESPEN ANDERSEN <EANDERSEN@HBS.HBS.HARVARD.EDU> Thu, 27 Feb 1992 22:58 EDT

I was involved in setting up rules for calculators etc. at exams a few years ago. The problems was: we wanted to permit students to use simple calculators on exams (as part of "regular exam tools", but did not want to make all exams open book because of students programming text etc. into small (and ever getting smaller) computers. At the same time we could not make the rules too technically oriented: the business school (in Norway) I worked for used retirees as exam proctors, and technical specificities were beyond their horizon.

Solution: devices allowed as long as they

- did not require AC
- did not make noise or could output to paper
- could not display more than 80 characters of text or numbers

The philosophy being that if the students really wanted to use devices that filled these specs on exams to cheat, they were welcome to: they would probably not derive any substantial benefit from it. (In fact, if a student goes through all the trouble of programming all the formulas into his HP-whatever, he (or she) will probably have learned them by heart and would not really need to have them programmed).

## Ke: Proposal for policy on calculator use during exams (Frankston 13.19)

Mark\_Jackson.wbst147@xerox.com <mjackson.wbst147@xerox.com> Fri, 28 Feb 1992 03:26:08 PST

> ... but that would reduce closed book exams to an abstract> exercise unrelated to actual practice.

Too late.

#### Ke: Calculator Use During Exams

Joe Morris <jcmorris@mwunix.mitre.org> Fri, 28 Feb 92 08:45:25 -0500

In <u>RISKS 13.19</u> several postings commented on the issues involved in the control of hand-held calculators during closed-book exams. The original posting is Bezenek (<u>RISKS 13.16</u>). Despite the recent interest shown by the postings, the issue isn't at all new.

My father, who for many years was the head of Tulane University's Physics department, refused to permit the use of slide rules by students taking exams for his undergraduate classes. While I don't necessarily agree that such an absolute ban was necessary, his reasoning was that while the slide rule (if correctly used...which wasn't a given assumption) could provide the correct digits in a problem, the user had the responsibility for keeping track of the decimal point...and since problems in physics involve huge ranges of exponents, the students would not develop the necessary recognition of "reasonableness" for the answers if they didn't work out the problems on paper. This is close to the issues raised by Cooper in <u>RISKS-13.19</u>.

There's been a story floating around so long that it may be urban legend, but supposedly there was an experiment several years ago in which a class was given an examination in which hand-held calculators were provided for their use. Unknown to the students, the calculators were rigged so that some of the calculations required on the examination would produce answers which were so far out of line that anyone paying the least attention to the results would have known that they were wrong. According to the story, only a minuscule number of the students caught the problem; the others blindly copied down the impossible results.

(Can anyone provide an authoritative citation for this? It's a good example even if it can't be verified, but it would be even better if it can be authenticated.)

Joe Morris

#### Ke: Calculator Use During Exams

<Mark.Kantrowitz@GLINDA.OZ.CS.CMU.EDU> Fri, 28 Feb 92 10:32:11 EST

My mother, a high school mathematics teacher, has a simple solution to the problem of calculator use during exams -- she maintains lists of the models her students are and are not allowed to use. At the beginning of the exam, she walks around the room and erases the memory of the calculators. (Most calculators have a short sequence of keystrokes which will erase all the memory.) A calculator which does symbolic integration, of course, is not allowed on an integration exam. Whenever a manufacturer debuts a new calculator, she buys or borrows one to evaluate it.

--mark

#### 🗡 DIAC-92

<douglas@atc.boeing.com> Mon, 10 Feb 92 14:20:21 PST

> DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING DIAC-92 Berkeley, California U.S.A May 2 - 3, 1992 8:30 AM - 5:30 PM

The DIAC Symposia are biannual explorations of the social implications of computing. In previous symposia such topics as virtual reality, high tech weaponry, national priorities, computers and education, affectionate technology, computing and the disabled, and many others have been highlighted. Our fourth DIAC Symposium, DIAC-92, will be held this Spring.

The first day will consist of individual presentations and panels on a variety of issues. The second day will consist of workshops that will be less formal and more highly interactive. Most of the workshops will be working sessions where output of some kind will be produced by the participants. Preliminary topics include:

- + Community and Global Electronic Networks
- + Computing in the 21st Century
- + Social Interactions in the MUD (Multi-User Dimension)
- + Work, Power, and Computers
- + Computing and Education
- + Civil Liberties in an Electronic Age

DIAC-92 will take place in 100 Genetic Plant Biology Building at the University of California at Berkeley. The GPB Building is in the northwest corner of the campus.

\*\*\*\*\*\*

PLEASE NOTE: Workshop Proposals are due March 1, 1992. Please contact Doug Schuler - dschuler@cs.washington.edu for "Call for Workshop Proposals."

To attend DIAC-92 send name, address, email address and registration form to:

DIAC-92 Registration, P.O. Box 2648, Sausalito, CA, 94966

Conference Fees: CPSR Member \$40 \_\_\_\_\_ (or AAAI, BCS, ACM SIGCAS, ACM SIGCHI) Non-member \$50 \_\_\_\_ New CPSR Membership (including DIAC Registration) \$80 \_\_\_\_ Student \$25 \_\_\_ Proceedings Only \$20 \_\_\_ Proceedings Only (foreign) \$25 \_\_\_ Additional Donation \_\_\_

Contact Doug Schuler, 206-865-3832 (work) or 206-632-1659 (home), or Internet dschuler@cs.washington.edu for additional information.

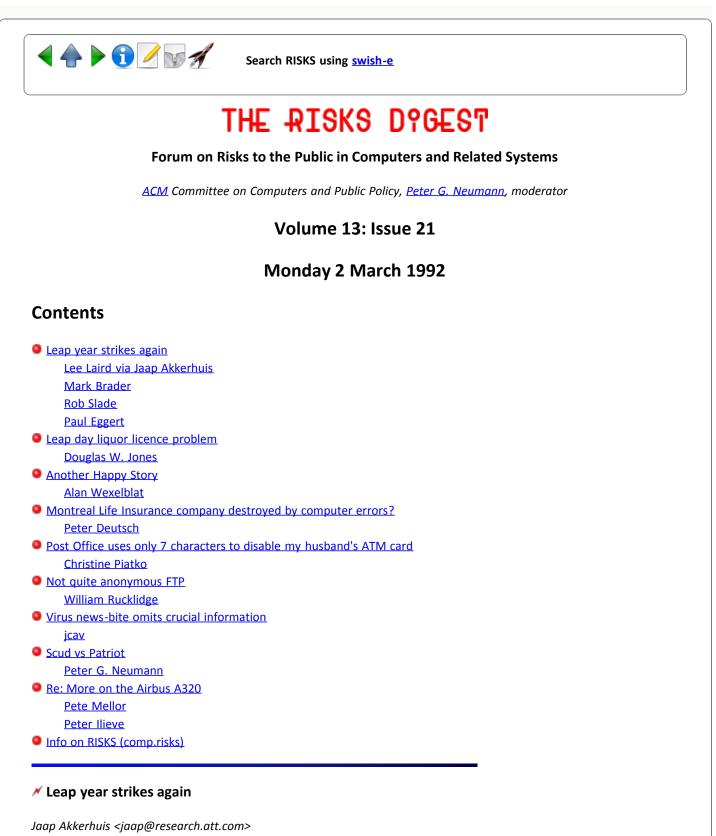
Sponsored by Computer Professionals for Social Responsibility P.O. Box 717 Palo Alto, CA 94301

DIAC-92 is co-sponsored by the American Association for Artificial Intelligence, and the Boston Computer Society Social Impact Group, in cooperation with ACM SIGCHI and ACM SIGCAS.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mon, 02 Mar 92 15:24:32 EST

The next complaint was sent to rec.radio.shortwave.

jaap (jaap@research.att.com)

From: Lee.Laird@f7009.n124.z1.fidonet.org (Lee Laird)

Newsgroups: rec.radio.shortwave Subject: forwarded from Date: 28 Feb 92 22:41:00 GMT Article-I.D.: ocitor.699420553.F00002 Posted: Fri Feb 28 17:41:00 1992 Sender: FredGate@ocitor.fidonet

thanks to the authors of Imail -- feb 29 has caused systems to crash worldwide since the mail tosser and handler does not recognize the date and locks up the system..

any outgoing dates with 29 feb also has that problem ... to overcome the problem and move the messages from my system i have had to set the date back and forward messages containing 29 feb ....

PLEASE DO NOT SEND REPLIES TO ME !!!!!!!

reply to those who i forwarded the message from... thanks. lee

\* Origin: -Com Port 1 DFW Amateur Radio BBS (214) 226-1181 (1:124/7009)

#### Risks of Leap Years and Dumb Digital Watches

Mark Brader <msb@sq.com> Sun, 1 Mar 1992 08:57:00 -0500

All right now, how many people reading this have watches that need to be set back a day because they went directly from February 28 to March 1-- and \*hadn't realized it yet\*?

(See <u>Risks-6.34</u> and 6.35 for the previous version of this message, and commentary on this and other leap-year problems.)

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

#### Re: Leaping Saturday

Rob Slade <rslade@cue.bc.ca> Mon, 2 Mar 92 14:20:02 PST

Working on my home computer on Saturday, I noticed something interesting. One computer was smart enough to handle the leap year with no problem. The other \*would not accept\* a February 29th date ... but was smart enough to know that March 1st was a Sunday.

Oh, well, I didn't get much done Saturday anyway ...

#### February 29th sneaks up again

Paul Eggert <eggert@bi.twinsun.com> Sun, 1 Mar 92 16:25:35 PST

As most RISKS readers know, February 29th is International Software Calendar Bug Day. Yesterday's quadrennial event found a bug in Prime's MAGSAV program that caused the program to fail promptly at midnight, as reported in the Usenet comp.sys.prime newsgroup by Peter Maurath. Ironically, the big day was a Saturday, and Prime's 800 number for software support doesn't work on weekends. (Message-ID <17174.29aee0a1@bclcl1.im.battelle.org>)

In the same forum, Richard H. Miller reported the usual workarounds: either use an older version of MAGSAV, or lie about the current date. He wrote, ``The indication is that it `snuck up on them' to paraphrase the Prime support person I talked with." (Message-ID <10383@gazette.bcm.tmc.edu>)

#### ✓ Leap day liquor licence problem

Douglas W. Jones,201H MLH,3193350740,3193382879 <jones@pyrite.cs.uiowa.edu> 28 Feb 92 18:57:40 GMT

The state of Iowa made a bit of a mistake this year. All liquor licences that should expire at the end of this Februrary expired today, on the 28th. The new licences only become valid on March first, so a large number of liquor stores, bars and restaurants have no liquor licence tomorrow (leap day). The state liquor control people have announced that this was due to a "computer error" and they promise not to enforce the law tomorrow, at least, not as it applies to those caught by this glitch.

Doug Jones jones@cs.uiowa.edu

#### Another Happy Story

<wex@pws.ma30.bull.com> Fri, 28 Feb 92 17:19:49 -0500

As people may know, the rock band U2 is starting a tour soon and is playing venues much smaller than the number of fans who would like to see them (13,000 seat arenas when they could easily fill 50,000+ seats).

The group has been going to extraordinary lengths to prevent ticket scalpers from getting tickets, including selling some venues by phone only. This has led to some real messes (as when they put the tickets for the Boston Garden show on sale. Half a million calls in the first hour).

One good computer-related side effect came to light the other day with the suspension of the manager of the Providence Civic Center. Seems this gentleman stands accused of deliberately overselling his arena with the extras going to scalpers. His scam was shut down after 150 extra tickets were sold. The oversell was detected by U2 people who were monitoring ticket sales from the central computer site in New York City.

So for once computer monitoring worked the way it should. And in a widely-

distributed system under high stress. Not too shabby.

Additionally, each ticket sale was verified to ensure that no one made duplicate orders. According to local radio reports, computer checks for duplication were made against "name, address, and credit card number." "450 duplicates were caught" and the orders cancelled after "human verification."

Again, I applaud appropriate use of technology -- the computer did the dumb brute work of finding possible matches and coughed up data to a human being for verification.

I'm sure someone will write in with information on what telephone services were denied during the deluge of calls, but hey, nothing's perfect.

--Alan Wexelblat, Bull Worldwide Information Systems, Billerica, MA phone: (508)294-6120 wexelblat.chi@xerox.com

#### Montreal Life Insurance company destroyed by computer errors?

Peter Deutsch <peterd@cc.mcgill.ca> Sat, 29 Feb 92 02:53:59 EST

A recent article by reporter Jay Bryan of the Montreal Gazette in the paper's business section made some extraordinary claims about the effect that bugs in a newly-installed integrated computer program had on the demise of a Montreal-based life insurance company.

It also has some things to say about both systems administration and systems integrators that might be of interest to the comp.risks readership.

#### The article begins:

"When Montreal Life Insurance Co., a growing, profitable insurer, decided to upgrade its main computer program 10 years ago, it jumped in with both feet. The new program, a kind called an integrated one, [yeah, right :-)] would tie together every aspect of the company's operations.

There was a small problem, though. The enormous program had been customized and installed in haste. Scattered through its one millions lines of computer instructions, there were a few undetected bugs. And since the system was integrated, every time a bug caused an error in one department's files, the error was immediately reflected in several other departments' files.

Within a year, Montreal Life was losing money. After three years, the company was near collapse. errors in commission cheques, for example, drove away most of the company's agents. The agents took their clients with them. When agents weren't underpaid, they were overpaid, which accounted for another \$1 million in losses.

Finally, what remained of Montreal Life was sold by its owners and most of the company's top managers lost their jobs....." This horror story is credited to two "systems auditors", Marshall Govindan and John Picard, who "... are determined to send a wake-up call to all those corporate leaders who think running a caompany's information system is just a housekeeping detail." Govindan apparently once worked for Montreal Life.

Despite its apparent "scare tactics" tone, the article goes on to discuss the need for proper systems management practices in which it makes a couple of good points about the need for suitable direction to systems staff from upper management. The point is made that "The systems people are basically a law unto themselves. They're accountable to nobody...this is because systems managers are treated as a kind of technological high priesthood. Their knowledge is considered so esoteric that top managers feel helpless to help them to the same standards of performance that are common in areas like marketing, operations or finance."

Apparently Govindan and Picard have written a book on the subject entitled "Manifesto on Informations Systems Control and Management", published by McGraw-Hill Ryerson. No further details of the book were given.

The article then describes a "success story", the Wal-Mart chain of retail stores, which apparently managed to speed checkout handling and minimize stocking with suitable, timely application of new technology.

The article finishes with a description of how a successful systems integrator works to bring up new technology and manage the transfer of new clients onto their systems while minimizing their disruptions. The conclusion was "All this [careful client handholding] is a 'pain in the neck' for systems people who might prefer to be doing something more technologically glamorous than sweating over every detail of every new installation...But from the perspective of the company, it means happy customers, rising sales and an assurance that the new system will produce steady profits instead of unexpected losses."

The article appeared in The Montreal Gazette, Saturday, February 22, 1992 on page C1 of the Business section, continuing onto page C4.

The risks are obvious. The tone is a tad alarmist, but if true, the tale of the demise of Montreal Life contains lessons for those who would rush into implementation of such mission critical software, and then insist on staying with such an obvious failure for as long as three years. I would therefore suspect that the tale of the fall of this company has a lot more that was left unsaid. Would any comp.risks readers have any more details on this? - peterd

#### Post Office uses only 7 characters to disable my husband's ATM card

Christine Piatko <piatko@cs.cornell.edu> Fri, 28 Feb 92 15:29:21 -0500

Speaking of the post office -- (I know that another Ithacan has complained to you about the way mail gets forwarded in Ithaca, but I thought I'd add my husband's mail-forwarding story.)

Last November my husband tried to use his ATM card over the Veterans' Day holiday weekend. The person in front of him successfully acquired cash from the ATM, but when he tried to get some money he got the uninformative error message "We're sorry, but we're unable to process your transaction right now." (This is the same message you might get when the machine is out of money, which often happens to this bank's machines during holiday weekends.) So he assumed he was just particularly unlucky that the person in front of him took the last of the cash in the machine.

The next day he tried at a different machine, again just after someone had taken out some money. He got the same message about not being able to complete the transaction. Frustrated, he tried small amounts of money, \$10, \$20, thinking perhaps the machine was out of particular bills. That didn't work either. We also have an ATM card for our joint account with the same bank. He tried that card and it worked fine.

(No, he didn't forget his PIN number and yes, the card was in one piece, and yes, this really does have to do with the Post Office.)

Puzzled, he called the bank after the holiday and asked them why the ATM card for his account didn't work. They looked up his record and said "Well, it's because your last statement got returned to us 'addressee unknown'." So part of the story is that the bank was stupid and didn't call to verify if he had moved (he hadn't), and locked out his ATM card. And part of the story is that my husband didn't realize he hadn't yet received his bank statement for the previous month. But the rest has to do with the way the Post Office forwards mail.

The bank gave him the statement that was still in its envelope with several yellow forwarding stickers on it. The hash function that the Post Office uses (at least in the Rochester branch of the Post Office) is first 3 numbers of the street address and the first 4 letters of the last name. My husband has a pretty common last name (Chang). Evidently, a Chang with a different first name who lived at a house numbered 216 on a completely different street (in a different section of Ithaca so the 9 digit zip codes didn't match either) recently moved out of Ithaca. Since my husband's name and address matched the 216CHAN hash function for forwarding, his statement was accidentally forwarded, and eventually got returned to the bank. Obviously, no one ever really compared the 2 addresses because the street names were very different.

All sorts of risks in this whole scenario, but what I can't understand is why the Post Office uses just these 7 characters for their hash function. Seems like there should be a way of using a character from the person's first name and the street name to make it work a little better. Our friend Jenn Turney had problems a few years ago when someone named Turner (with a different first name, and different street name, but the same 3 digit house number) moved. Scanning the phone book, I wonder if Andy Chan, Kenneth Chan or Sak Chanthanak (all with 216 house numbers) have had any problems with their mail being forwarded...

Christine Piatko (piatko@cs.cornell.edu)

# Not quite anonymous FTP

William Rucklidge <wjr@cs.cornell.edu> Sat, 29 Feb 92 18:04:14 -0500

The recent MBDF-A virus which was (allegedly) uploaded to SUMEX-AIM by two Cornell students shows a possible risk: it seems likely that the students were tracked down via examination of machine logs, both at Stanford and at Cornell. They might have been aware of the "last" log, showing who was logged in to what machine when, but probably were not aware that "anonymous" ftp accesses are routinely logged. While the username which you provide can, of course, be anything, it is much more difficult to disguise the source of the FTP transaction, and this can be logged.

The risk is not so much that the logs are made, but more that the service is presented as "anonymous", leading people to believe that it actually is.

William Rucklidge wjr@cs.cornell.edu

#### ✓ Virus news-bite omits crucial information

<jcav@midway.uchicago.edu> Mon, 02 Mar 92 15:30:55 -0600

This morning I happened to catch newsman Charles Osgood's "The Osgood File" on the local CBS AM all-news station. "The Osgood File" is a two-minute long daily radio "column" in which Mr. Osgood talks about something in the news that interests him. Today the topic was the "Michaelangelo" computer virus. Mr. Osgood spoke repeatedly of the danger to "your computer", and had a brief interview with a computer consultant who also spoke of the danger to "computers". AT NO TIME DURING THE PIECE DID ANYONE MENTION THAT THE VIRUS AFFECTS MS-DOS CLONE MACHINES ONLY. The gist of the piece was that viruses are bad and that all computers are in horrible danger of losing their files on the fateful anniversary this Friday.

I called Mr. Osgood's office in New York City and spoke to a woman who was very pleasant to me, and seemed surprised that that particular bit of information had not been included. I'm not sure I was forceful enough in stating how crucial the missing information was to the story. I still can't believe that it was omitted.

#### Scud vs Patriot

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 2 Mar 92 14:57:57 PST

James Paul just sent me a copy of a report to the Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives, from the US General Accounting Office, entitled

Patriot Missile Defense: Software Problem Led to System Failure at

Dhahran, Saudi Arabia. GAO/IMTEC-92-26, February 1992

along with letters from the Subcommittee Chairman, Congressman Howard Wolpe (Michigan) to Richard Cheney, John Conyers (Chairman of the Committee on Government Operations) and Les Aspin (Chairman of the Committee on Armed Services). If any of you want to see the report and/or the letters, please contact James Paul at paul@Nova.House.Gov or call 202-226-3639. You may also get a copy of the report directly from the US GAO, 202-275-6241; single copies of the report are free.

The details are mostly known to RISKS readers. Appendix II shows the effect of extended run time, with a .3433 second time inaccuracy over 100 hours, and a shift of 687 meters in range gate.

[Science Committee staffer James Paul was the author of the remarkable 1989 report, Bugs in the Program: Problems in Federal Government Computer Software Development and Regulation.]

[I presume you all saw the Scud item in <u>RISKS-13.19</u>.]

# Ke: More on the Airbus A320 (Marchant-Shapiro, <u>RISKS-13.19</u>)

Pete Mellor <pm@cs.city.ac.uk> Fri, 28 Feb 92 12:42:25 GMT

> Any comments from qualified persons?

My only qualification is that I have read the interim report of the commission of enquiry into the Strasbourg crash, and a few other documents.

> MOST 320 aircraft have an alarm that informs the pilot that s/he
 > is flying too low, but France does not require this alarm and so aircraft
 > sold to and/or operated by French companies do not have this alarm installed.

The Ground Proximity Warning System (GPWS) is standard equipment, and is mandated by international regulations. Air Inter, which operated the A320 which crashed at Strasbourg, are a purely domestic airline. Since their aircraft do not fly outside France, they are not covered by the international rules.

Air Inter took a deliberate policy decision many years ago \*not\* to use GPWS, since such systems are (or were then) prone to giving false alarms. They argued that, in any case, their pilots were highly familiar with the terrain around the airports they served, and so didn't need GPWS.

In its interim report, the commission of enquiry has been \*very\* careful not to draw any conclusions, or even entertain any theories, about the cause(s) of the crash. However they are aware that the use of GPWS would have made an accident of this type less likely, and the second of their three interim recommendations is that the French national regulations are amended as soon as possible to make the installation of GPWS mandatory on all aircraft large enough to carry one, including those used only on domestic routes. Note that international carriers, such as Air France, \*are\* covered by international regulations, and have always had GPWS in their A320s.

> If so, this points to a particularly interesting human interface problem -> perhaps the A320 tends to drop faster than other aircraft, but, since there
> is no alarm, [some] pilots do not realize what is happening until they're
> too low to do anything about it.

The human interface problem which most concerns the commission, and which is the subject of their first interim recommendation, is the possibility of confusion between the two modes of descent: "Vertical Speed" and "Flight Path Angle". For a detailed description of how this confusion could arise, see Robert Dorsett's excellent description of the Flight Management System (FMS) in <u>RISKS-13.11</u>. One possible effect of the pilot selecting the wrong mode is that the aircraft would descend much faster than intended. Apart from that situation, as far as I know the A320 drops neither faster nor slower than any other airliner.

On 28th January, the DGAC (French equivalent of the FAA) warned users of the A320 about the danger of confusing the two modes, and immediately put in place procedures and documentation to prevent this happening. The French Minister of Transport has directed the DGAC to monitor the effectiveness of these temporary measures carefully, and told them to direct Airbus Industrie, who manufacture the A320, to produce a detailed plan (within one month) of modifications to that particular part of the pilot-FMS interface. The implementation and certification of the modified FMS will obviously take much longer.

Again, the report stresses that this recommendation does \*not\* imply that the commission have concluded that confusion of descent modes is the cause, or part of the cause, of the Strasbourg crash.

The commission's third interim recommendation (again backed up by the Minister) is to make the automatic emergency radio beacon less likely to be damaged in a crash. At Strasbourg it was destroyed, and this has been suggested as one reason why it took rescue teams so long to get to the crash site.

The Minister added a fourth directive to the DGAC to look into more rugged flight recorders, and improved protection for them. At Strasbourg, the Digital Flight Data Recorder (DFDR) was fried to a crisp, and the Cockpit Voice Recorder (CVR) and Quick Access Recorder (QAR) were damaged, but still readable in parts. In the last three years there have been five accidents in which the recorders have been destroyed, according to the Minister's statement last Monday.

Recorders and emergency beacons are useful only after you've already crashed the 'plane, of course.

Whether the crash could have been averted if a GPWS had been fitted is obviously still an open question. It would depend on the length of time before impact at which the warning would have been given, and I do not have this information right now. There is, however, another system, the radiosonde alarm, which gives a simulated voice warning as the aircraft passes down through certain thresholds of altitude, measured by a radio beam reflected from the ground. The top threshold is 200ft.

This is separate from the GPWS, and \*was\* in use on the Strasbourg A320. The transcript of the CVR shows a single radiosonde announcement of "Two hundred feet". Although no time stamp is shown on the CVR transcript, this is the last thing that appears, and seems to have occurred a mere second or so before impact.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

#### Interim commission of inquiry report into Strasbourg A320 crash

Peter Ilieve <peter@memex.co.uk> Mon, 2 Mar 92 13:26:14 GMT

On 25 Feb 1992, the papers here reported on the interim report of the French commission of inquiry into the Strasbourg A320 crash. Although they emphasise that they have not concluded what caused the crash it seems they are leaning towards the confusion of the vertical speed and flight path angle modes of descent as desribed by Robert Dorsett in <u>risks 13.11</u>. To show how confusing this is, the reports in the Times and the Independent (2 quality UK papers) contradict each other on the mode that the pilots should have been using.

>From the Independent:

The French government yesterday ordered modifications to the instruments of the Airbus A320, one of which crashed near Strasbourg last month.

Paul Quil\`es, the Transport Minister, said the changes would affect the systems controlling descent. [He wanted Airbus] to report within one month on how it would carry out the modifications. ...

The commission ... recommended to ``the ergonomics of the aircraft-crew interface linked to the `Vertical Speed' and `Flight Path Angle' modes''. On the A320 ... pilots select a pattern by pressing a button on the instument panel. The choice is determined by pressing the button once or twice. The Flight Path Angle would have been normal for the Strasbourg approach.

[end quote]

The story goes on to say that the government were ordering that GPWS should be installed in all aircraft. Air Inter did not have this as they had had reliability and false alarm problems with them.

It also mentions the problem of slippage between the A320's map display and the position on the ground. Air France and Air Inter had stopped using this after a pilot flying into Bordeaux noticed a difference between indicated and real positions. The commission are not saying that this problem was linked to the Strasbourg crash but the report says that the cockpit voice recorder indicates that the pilots were concentrating on their lateral position just before the crash.

#### >From the Times:

The manufacturers of the A320 ... are to seek new ways of making their jets ``pilot-proof" and preventing crews from mistaking their flight path angle for their speed of descent.

Air accident investigators ... have yet to find the precise cause ... but their preliminary report suggests that the pilots could have programmed the computer wrongly because of confusion over the role of one of the instruments. ...

As they approached Strasbourg and were told to make a standard descent, it is now thought likely that they ordered the aircraft to descent at an angle rather than at so many feet per minute.

#### [end quote]

The Times report is written with much more emphasis on pilot error. It doesn't mention the government order to Airbus to change things or the map problem.

On Sunday 1 March the Sunday Times, a 'heavyweight' (in both senses of the word, 9 sections and still growing) UK paper had a piece in its business section headed 'Airbus has worst record'.

Airbus Industrie, the European aircraft consortium, has suffered a new setback with the revalation that its A320 currently has the worst accident record of large passenger jets registered in Britain.

An insurance industry report shows that crashes involving the plane, the most advanced flown by airlines, have led to a higher death rate among passengers than on aircraft designed nearly 25 years ago.

•••

Paul Hayes, director of Airclaims, the aviation consultancy which drew up the report, said it was too soon to draw conclusions over the safety of the four-year-old A320. ``Its loss rates are worse at the moment but this does not mean that it is a dangerous aircraft. If these are maintained over a longer time, however, it may indicate a serious problem for ASirbus," he said.

The report examines the loss and fatality rates for all jet and turbo-prop aircraft over the past five years. It shows that one person was killed on A320s for every 331,900 carried, compared with one for every 1,401,100 on DC10s, the next worse. If the French disaster was included, the A320 figure would drop to one for every 270,000, a record more than eight times worse than the average for its generation of jets.

The aircraft is shown to have had a fatal accident for every 241,700 landings, seven times worse than the performance of the Boeing 757, one of its main rivals. The older A300 and A310, which do not use the contoversial fly-by-wire system, have not had a fatal accident.

Airbus said it was unfortunate that aircraft crashes were remembered for the type of plane involved rather than the cause. ``There have been three crashes and in the first two it was quite clear that the aircraft was not at fault," a spokeswoman said.

#### [end quote]

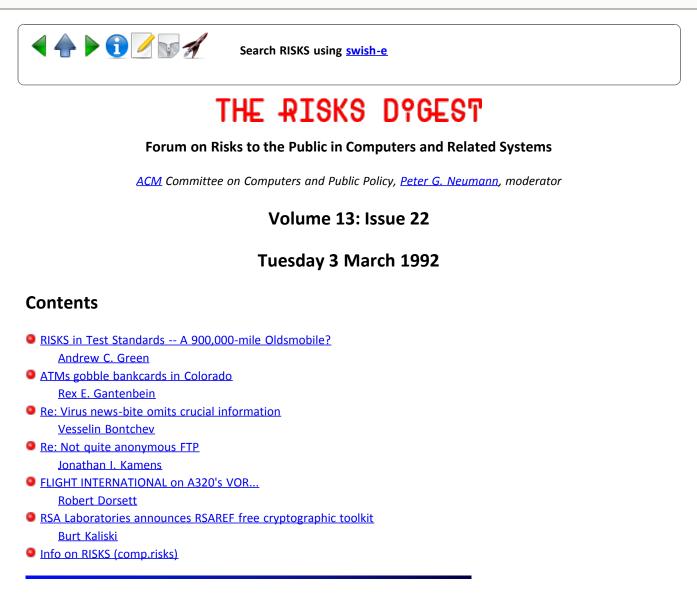
Airbus' comments in the last paragraph of this report seem suspect to me.

Unless you assume that the pilots flying A320s are more stupid than average, then if pilots have more crashes in A320s than other planes, even if the cause is officially `pilot error', there must be something about the plane that makes errors more likely.

Peter Ilieve peter@memex.co.uk



Report problems with the web pages to the maintainer



# KISKS in Test Standards -- A 900,000-mile Oldsmobile?

<acg@hermes.dlogics.com> Tue, 03 Mar 1992 08:34:59 CST

Here in northern Illinois, we must have our cars tested periodically (usually once a year) for exhaust emissions. The test operator has to enter the current mileage of the vehicle into the computer, which then sets the proper standards that the vehicle must meet. High-mileage cars are permitted to spew out slightly more pollutants (within reason) than low-mileage ones. Up until this year, the operator could only enter five digits, so any car exceeding 100,000 miles on the odometer was listed at 99,000. This year, they've revised the system to handle six digits, and things got interesting.

Last week I brought my 90,000-mile 1982 Oldsmobile in for its test. The test operator said, "What's the first two digits on your mileage?" "Nine, Zero", I replied. He punched it in and the test proceeded.

I wondered at the time how they deal with cars having SEVEN digit odometers. Seems like the operator would have to know whether to punch in a leading zero, but from the wording of the question, it sounded like he could only enter two digits no matter what. The owner of a 90,000-mile Honda (whose odometer reads "090,000.0") might have answered "Zero, Nine" to that question, and get stuck trying to meet a 9,000-mile emission standard instead of a 90,000-mile setting. On the other hand, maybe I would be the lucky recipient of a 900,000-mile testing standard? If my car fails THAT, I thought, I'm definitely getting a tuneup.

Well, the car passed with flying colors, and as I drove off, I glanced at the printout of results given to me with my new 1-year emissions sticker. Sure enough, the indicated test mileage read "900,000", complete with the comma in the middle.

Other than the obvious RISK, that of flunking the test because of a goofed-up mileage entry, I wonder if the odometer reading for emissions testing is tracked from year to year. Data on the printout shows that the computer is indeed tied into the registration information for the car. The mileage IS listed on the car's Title of Ownership to catch rollbacks between purchase and later sale, but I don't know if any discrepancies are flagged automatically. Hope not, anyway. I wonder if the operator who gets the test mileage correct next year, say at 99,000 miles, will get a message from the computer asking what happened to the other 801,000?

Andrew C. Green, Datalogics, Inc., 441 W. Huron, Chicago, IL 60610 (312) 266-4431 Internet: acg@dlogics.com UUCP: ..!uunet!dlogics!acg

#### ATMs gobble bankcards in Colorado

"Rex E. Gantenbein 307-766-4226" <REX@corral.uwyo.edu> Mon, 2 Mar 1992 16:20 MST

Source: Denver Post, 19 Feb 1992

About 1,000 Colorado ATM users had their Visas and Mastercards abruptly terminated in February by an out-of-control computer system.

For 90 minutes during the President's Day weekend, the Rocky Mountain Bankcard System software told ATMS around the state to eat the cards instead of dishing out cash or taking deposits. The "once-in-a-decade" glitch went unnoticed because it occurred as programmers were patching in a correction to a different problem.

The company is rushing new plastic and letters of apology to customers who got terminated.

#### Ke: Virus news-bite omits crucial information

Mr. News <news@rzsun2.informatik.uni-hamburg.de> Tue, 3 Mar 92 10:30:29 +0100

risks@csl.sri.com writes:

> AT NO TIME DURING THE PIECE DID ANYONE MENTION THAT THE VIRUS> AFFECTS MS-DOS CLONE MACHINES ONLY.

Sigh... Sorry, but this is FALSE! The Michelangelo virus attacks any IBM PC compatible computers. There is no need that they are MS-DOS machines. You can get a 80386 and install only Xenix on it, without any MS-DOS partitions. The virus will still infect it and will destroy the information on the hard disk on March 6. Of course, Xenix won't be able to boot after the infection, but this is another story...

Vesselin Vladimirov Bontchev Virus Test Center, University of Hamburg Bontchev@Informatik.Uni-Hamburg.De Fachbereich Informatik - AGN, rm. 107 C Tel.:+49-40-54715-224, Fax: -226 Vogt-Koelln-Strasse 30, D-2000, Hamburg 54

#### Ke: Not quite anonymous FTP (Rucklidge, <u>RISKS-13.21</u>)

"Jonathan I. Kamens" <jik@pit-manager.MIT.EDU> Tue, 3 Mar 92 10:21:19 -0500

The risk is not so much that the logs are made, but more that the service is presented as "anonymous", leading people to believe that it actually is.

Not convinced. It is standard operating procedure to ask users of anonymous ftp to specify their E-mail address when prompted for a password. In fact, pretty much every document I've seen that describes anonymous ftp mentions this practice, and explains that the purpose of it is to allow system administrators to monitor the usage of anonymous ftp.

Given such a widespread, accepted convention, it seems clear to me that users of anonymous ftp have no reason to expect their usage to be completely anonymous. Furthermore, if the provide a fake or bogus E-mail address when prompted for an ftp password, they are doing something considered anti-social on the Internet, and I think it is completely reasonable for the addresses of connecting sites to be logged in case it becomes necessary to follow up on such anti-social behavior.

I don't see any risk here. I see a system that worked the way it was designed to work, and the users who were caught allegedly doing something wrong had no "right" to expect otherwise.

Jonathan Kamens jik@MIT.Edu

#### FLIGHT INTERNATIONAL on A320's VOR...

Robert Dorsett <rdd@cactus.org> Mon, 2 Mar 92 15:32:34 CST

Since the Air Inter A320 crashed January 20, there have been a number of comments on shifted map displays, and that Lufthansa had banned the use of VOR/DME approaches for the previous year.

Obligatory technolingo:

A VOR is a ground-based electronic broadcasting station, which transmits radial "spokes." These range from 0 to 359 degrees. An airplane can check to see which "spoke" it's on; this data can then be used for navigation purposes. This is contrasted with an NDB (non-directional station), which, like an AM radio station, simply broadcasts in all directions; direction-finding equipment on board the airplane can then be used to find it. VOR's are generally more reliable over longer ranges, and less susceptible to interference. The operational difference is that airplane instrumentation points TO an NTB, but shows what radial the airplane is ON with a VOR.

Comments in brackets []. Some are sarcastic, some are technical clarifications; there are a few mistakes in this.

>From FLIGHT INTERNATIONAL, "New VOR antenna will solve A320 problem", Feb. 19, 1992, p. 10:

"Airbus Industrie, workin with Lufthansa, has developed a new VOR (VHF omnirange) antenna for its A320s.

"The resulting modification programme will overcome the occasional poor aircraft reception of VOR beacon signals, which had caused Lufthansa, in September 1991, to suspend VOR/DME (distance measuring equipment) airfield approaches in its A320s.

"On 8 February Air France and Air Inter took a voluntary decision to suspend VOR/DME approaches in their A320s because of an incident in an Air Inter A320 on approach to Bordeaux airport three days earlier.

"The symptom for the Lufthansa problem was oscillation of the VOR indicator in the A320 cockpit displays. Also, the Bendix DME equipment in Boeing 747-400s--the same as in the A320s--had once shown a fault which had been reproduced on the test bench.

"Work at Bendix has not yet produced a modificaiton, but the fault has not recurred in the 747 or occurred ever in Lufthansa's A320s. Air France uses Bendix VOR/DME, Air Inter has Collins.

"Airbus senior vice-president of engineering, Bernard Ziegler, says that the antenna problem was related to the position of metal lightning-protection strips in the composite aerial.

"In the Air Inter incident on 5 February, the A320 captain, carrying out a VOR/ DME procedure for Bordeaux, but flying manually in perfect visual conditions, noticed that the flight management system (FMS)-produced map on his navigation display was displaced. Ziegler confirms it was displaced by 2.2 cm (1.2 nm), pointing out that such a degree of displacement, while unsatisfactory, was within the published system accuracy. [!!!] [!]

"Lufthansa emphasizes that it had not experienced map displacement, only VOR indicator oscillation.

"Lufthansa's letdown procedure involves one pilot flying to the compass arc/

map display, the other to the VOR compass rose display, to enable cross-checking. The raw VOR/DME data on both displays is correct even if the map is displaced. [but does anyone use the raw data when the map is so much more convenient?]

"Ziegler says the Bordeaux map display displacement was caused partly by an Air Inter database error entered in the aircraft's FMS, which produces the display map from its integral inertial navigation system (INS) [actually, ADIRS]. The INS [FMS] depends on VOR/DME for its accuracy updating. If fewer than two DMEs are in range (and during descent this often occurs), then the INS [FMS] updates using a co-located VOR/DME. The Air Inter database says the Bordeaux VOR and DME are co-located when they are not [!], so the FMS was cleared to updated, using incorrect information and affecting the map. [GIGO rules!]

"The navigation display, Ziegler says, displays the FMS update sources at all times: 'If you see that the source is VOR/DME and your VOR needle is oscillating, obviously you know you can expect map shift.' [obviously.]

"The French Direction Generale de l'Aviation Civile (DGAC) will not ban A320 VOR/DME letdowns, but empahsises the need to crosscheck the map displays with the raw navigation data available.

"The DGAC also points out that there is no evidence of any connection between the Bordeaux event and the Air Inter A320 crash near Starsbourg on 20 January. The authority has, however, warned all A320 crews to be careful when they select the autopilot descent mode, because there is a possibility that the Strasbourg crew may have selected a steep 3300 fpm (16.7 m/s) rate of descent when they meant to select the shallower 3.3 degree angle of descent.

Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd

#### KRSA Laboratories announces RSAREF free cryptographic toolkit

Burt Kaliski <burt@RSA.COM> Mon, 2 Mar 92 16:27:21 PST

> RSAREF(TM): A Cryptographic Toolkit for Privacy-Enhanced Mail

RSA Laboratories (A division of RSA Data Security, Inc.) March 2, 1992

This document copyright (C) 1992 RSA Laboratories, a division of RSA Data Security, Inc. License is granted to reproduce, copy, post, or distribute in any manner, provided this document is kept intact and no modifications, deletions, or additions are made.

WHAT IS IT?

RSAREF is a cryptographic toolkit designed to facilitate rapid deployment of Internet Privacy-Enhanced Mail (PEM) implementations. RSAREF represents the fruits of RSA Data Security's commitment to the U.S. Department of Defense's Advanced Research Projects Agency (DARPA) to provide free cryptographic source code in support of a PEM standard. RSA Laboratories offers RSAREF in expectation of PEM's forthcoming publication as an Internet standard.

Part of RSA's commitment to DARPA was to authorize Trusted Information Systems of Glenwood, MD, to distribute a full PEM implementation based on RSAREF. That implementation will be available this spring.

RSAREF supports the following PEM-specified algorithms:

- RSA encryption and key generation, as defined by RSA Laboratories' Public-Key Cryptography Standards (PKCS)
- o MD2 and MD5 message digests
- o DES (Data Encryption Standard) in cipher-block chaining mode

RSAREF is written in the C programming language as a library that can be called from an application program. A simple PEM implementation can be built directly on top of RSAREF, together with message parsing and formatting routines and certificate-management routines. RSAREF is distributed with a demonstration program that shows how one might build such an implementation.

The name "RSAREF" means "RSA reference." RSA Laboratories intends RSAREF to serve as a portable, educational, reference implementation of cryptography.

#### WHAT YOU CAN (AND CANNOT) DO WITH RSAREF

The license at the end of this note gives legal terms and conditions. Here's the layman's interpretation, for information only and with no legal weight:

- You can use RSAREF in personal, noncommercial applications, as long as you follow the interface described in the RSAREF documentation. You can't use RSAREF in any commercial (moneymaking) manner of any type, nor can you use it to provide services of any kind to any other party. For information on commercial licenses of RSAREF-compatible products, please contact RSA Data Security.
- You can distribute programs that interface to RSAREF, but you can't distribute RSAREF itself. Everyone must obtain his or her own copy of RSAREF. (However, free licenses to redistribute RSAREF are available. For information, please send electronic mail to <rsaref-administrator@rsa.com>.)
- 3. You can modify RSAREF as required to port it to other operating systems and compilers, as long as you give a copy of the results to RSA Laboratories. You can't otherwise

change RSAREF.

4. You can't send RSAREF outside the United States, or give it to anyone who is not a United States citizen and doesn't have a "green card." (These are U.S. State and Commerce Department requirements, because RSA and DES are export-controlled technologies.)

The restrictions on the distribution of RSAREF are the consequence of export-control law. Similar constraints are placed on those redistributing RSAREF under free license from RSA Laboratories. Without the export-control law, RSAREF would be available by anonymous FTP.

#### HOW TO GET IT

To obtain RSAREF, read the license at the end of the note and return a copy of the "acknowledgement and acceptance" paragraph by electronic mail to <rsaref-administrator@rsa.com>.

RSAREF is distributed by electronic mail in a UNIX(TM) "uuencoded" TAR format. When you receive it, store the contents of the message in a file, and run your operating system's "uudecode" and TAR programs.

For example, suppose you store the contents of your message in the file 'contents'. You would run the commands:

RSAREF includes about 60 files organized into the following subdirectories:

docdocumentation on RSAREF and RDEMOinstallmakefiles for various operating systemsrdemoRDEMO demonstration programsourceRSAREF source code and include filestesttest scripts for RDEMO

#### USERS' GROUP

RSA Laboratories maintains the electronic-mail users' group <rsaref-users@rsa.com> for discussion of RSAREF applications, bug fixes, etc. To join the user's group, send electronic mail to <rsaref-users-request@rsa.com>.

#### REGISTRATION

RSAREF users who register with RSA Laboratories are entitled to free RSAREF upgrades and bug fixes as soon as they become available and a 50% discount on selected RSA Data Security products. To register, send your name, address, and

telephone number to <rsaref-registration@rsa.com>.

# INNOVATION PRIZES

RSA Laboratories will award cash prizes for the best applications built on RSAREF. If you'd like to submit an application, or want to be on the review panel, please send electronic mail to <rsaref-administrator@rsa.com>.

# PUBLIC-KEY CERTIFICATION

RSA Data Security offers public-key certification services conforming to forthcoming PEM standards. For more information, please send electronic mail to <pem-info@rsa.com>.

# OTHER QUESTIONS

If you have questions on RSAREF software, licenses, export restrictions, or other RSA Laboratories offerings, send electronic mail to <rsaref-administrator@rsa.com>.

## AUTHORS

RSAREF was written by the staff of RSA Laboratories with assistance from RSA Data Security's software engineers. The DES code is based on an implementation that Justin Reyneri did at Stanford University. Jim Hwang of Stanford wrote parts of the arithmetic code under contract to RSA Laboratories.

## ABOUT RSA LABORATORIES

RSA Laboratories is the research and development division of RSA Data Security, Inc., the company founded by the inventors of the RSA public-key cryptosystem. RSA Laboratories reviews, designs and implements secure and efficient cryptosystems of all kinds. Its clients include government agencies, telecommunications companies, computer manufacturers, software developers, cable TV broadcasters, interactive video manufacturers, and satellite broadcast companies, among others.

RSA Laboratories draws upon the talents of the following people:

- Len Adleman, distinguished associate Ph.D., University of California, Berkeley; Henry Salvatori professor of computer science at University of Southern California; co-inventor of RSA public-key cryptosystem; co-founder of RSA Data Security, Inc.
- Taher Elgamal, senior associate Ph.D., Stanford University; director of engineering at RSA Data Security, Inc.; inventor of Elgamal public-key cryptosystem based on discrete logarithms

Marty Hellman, distinguished associate - Ph.D., Stanford University;

professor of electrical engineering at Stanford University; co-inventor of public-key cryptography, exponential key exchange; IEEE fellow; IEEE Centennial Medal recipient

Burt Kaliski, chief scientist - Ph.D., MIT; former visiting assistant professor at Rochester Institute of Technology; author, Public-Key Cryptography Standards; general chair, CRYPTO '91

Cetin Koc, associate - Ph.D., University of California, Santa Barbara; assistant professor at University of Houston

Ron Rivest, distinguished associate - Ph.D., Stanford University; professor of computer science, MIT; co-inventor, RSA public-key cryptosystem; co-founder, RSA Data Security, Inc.; member, National Academy of Engineering; director, International Association for Cryptologic Research; program co-chair, ASIACRYPT '91

#### ADDRESSES

RSA Laboratories	RSA Data Security, Inc.
10 Twin Dolphin Drive	100 Marine Parkway
Redwood City, CA 94065	Redwood City, CA 94065
USA U	SA

(415) 595-7703	(415) 595-8782
(415) 595-4126 (fax)	(415) 595-1873 (fax)

PKCS, RSAREF and RSA Laboratories are trademarks of RSA Data Security, Inc. All other company names and trademarks are not.

RSA LABORATORIES PROGRAM LICENSE AGREEMENT

RSA LABORATORIES, A DIVISION OF RSA DATA SECURITY, INC. ("RSA"), IS WILLING TO LICENSE THE "RSAREF" PROGRAM FOR YOUR USE ONLY ON THE TERMS AND CONDITIONS SET FORTH BELOW. YOUR ACKNOWLEDGEMENT AND ACCEPTANCE OF THESE TERMS AND CONDITIONS BY RETURN ELECTRONIC TRANSMISSION IS REQUIRED PRIOR TO DELIVERY TO YOU OF THE RSAREF PROGRAM.

- LICENSE. RSA is willing to grant you a non-exclusive, non-transferable license for the "RSAREF" program (the "Program") and its associated documentation, subject to all of the following terms and conditions, but only:
  - a. to use the Program on any computer in your possession, but on no more than one computer at any time;
  - b. to make one copy of the Program for back-up purposes only;
  - c. to incorporate the Program into other computer programs only through interfaces described in the RSAREF Library

Reference (the file "rsaref.txt" which accompanies the Program) (any such incorporated portion of the Program to continue to be subject to the terms and conditions of this license) both solely for your own personal or internal use or to create Application Programs; and

d. to modify the Program for the purpose of porting the Program to any other operating systems and compilers, but only on the conditions that: (i) you do not alter any Program interface, except with the prior written consent of RSA; and (ii) you provide RSA with a copy of the ported version of the Program by electronic mail.

"Application Programs" are programs which interface with the Program but which do not incorporate all or any portion of the Program, whether in source code or object code form.

- 2. LIMITATIONS ON LICENSE.
  - a. RSA owns the Program and its associated documentation and all copyrights therein. YOU MAY NOT USE, COPY, MODIFY OR TRANSFER THE PROGRAM, IN EITHER SOURCE CODE OR OBJECT CODE FORM, ITS ASSOCIATED DOCUMENTATION, OR ANY COPY, MODIFICATION OR MERGED PORTION THEREOF, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT OR WITH THE PRIOR WRITTEN CONSENT OF RSA. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, YOU MAY NOT PLACE THE PROGRAM ON ANY ELECTRONIC BULLETIN BOARD SYSTEM (BBS) OR MAKE THE PROGRAM AVAILABLE THROUGH ANY FILE TRANSFER PROTOCOL (FTP). YOU MUST REPRODUCE AND INCLUDE RSA'S COPYRIGHT NOTICES ON ANY COPY OR MODIFICATION, OR ANY PORTION THEREOF, OF THE PROGRAM AND ITS ASSOCIATED DOCUMENTATION.
  - b. The Program is to be used only in connection with a single computer. You may physically transfer the Program from one computer to another, provided that the Program is used in connection with only one computer at any given time. You may not transfer the program electronically from one computer to another over a network except in connection with your own personal or internal use of the Program. You may not distribute copies of the Program or its associated documentation. IF YOU TRANSFER POSSESSION OF ANY COPY, MODIFICATION OR MERGED PORTION OF THE PROGRAM, WHETHER IN SOURCE CODE OR OBJECT CODE FORM, OR ITS ASSOCIATED DOCUMENTATION TO ANOTHER PARTY, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE, YOUR LICENSE SHALL BE AUTOMATICALLY TERMINATED.
  - c. The Program is to be used only for non-commercial purposes. You may not use the Program to provide services to others for which you are compensated in any manner. You may not license, distribute or otherwise transfer the Program or any part thereof in any form, whether you receive compensation or not.

- d. You may not translate the Program into any other computer language.
- e. You may not incorporate the Program into other programs through interfaces other than the interfaces described in the RSAREF Library Reference.
- 3. NO WARRANTY OF PERFORMANCE. THE PROGRAM AND ITS ASSOCIATED DOCUMENTATION ARE LICENSED "AS IS" WITHOUT WARRANTY AS TO THEIR PERFORMANCE, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PROGRAM IS ASSUMED BY YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU (AND NOT RSA OR ITS DISTRIBUTOR) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 4. LIMITATION OF LIABILITY. EXCEPT AS EXPRESSLY PROVIDED FOR IN SECTION 5 HEREINUNDER, NEITHER RSA NOR ANY OTHER PERSON WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE PROGRAM SHALL BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO ANY DAMAGES FOR LOST DATA, RE-RUN TIME, INACCURATE INPUT, WORK DELAYS OR LOST PROFITS, RESULTING FROM THE USE OF THE PROGRAM OR ITS ASSOCIATED DOCUMENTATION, EVEN IF RSA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- 5. PATENT INFRINGEMENT INDEMNITY. RSA shall indemnify and hold you harmless from any and all liability, damages, costs or expenses (including reasonable attorneys' fees) which you may incur as the result of any claim that the unmodified Program infringes a United States patent in the field of cryptography. RSA shall have no obligation to you pursuant to this Section 5 unless: (i) you give RSA prompt written notice of the claim; (ii) RSA is given the right to control and direct the investigation, preparation, defense and settlement of the claim; and (iii) the claim is based on your use of the unmodified Program in accordance with this license. THIS SECTION 5 SETS FORTH RSA'S ENTIRE OBLIGATION AND YOUR EXCLUSIVE REMEDIES CONCERNING CLAIMS FOR PROPRIETARY RIGHTS INFRINGEMENT.

NOTE: PORTIONS OF THE PROGRAM PRACTICE METHODS DESCRIBED IN AND ARE SUBJECT TO U.S. PATENTS #4,218,582 AND #4,405,829, ISSUED TO LELAND STANFORD JR. UNIVERSITY AND MASSACHUSETTS INSTITUTE OF TECHNOLOGY RESPECTIVELY. EXCLUSIVE LICENSING RIGHTS ARE HELD BY PUBLIC KEY PARTNERS OF SUNNYVALE, CALIFORNIA.

6. RESTRICTIONS ON FOREIGN RESHIPMENT. THIS LICENSE IS EXPRESSLY MADE SUBJECT TO ANY LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT FROM THE UNITED STATES OF AMERICA OF THE PROGRAM OR OF ANY INFORMATION ABOUT THE PROGRAM WHICH MAY BE IMPOSED FROM TIME TO TIME BY THE GOVERNMENT OF THE UNITED STATES OF AMERICA. YOU MAY NOT EXPORT OR REEXPORT, DIRECTLY OR INDIRECTLY, THE PROGRAM OR INFORMATION PERTAINING THERETO.

- 7. TERM. The license granted hereunder is effective until terminated. You may terminate it at any time by destroying the Program and its associated documentation together with all copies, modifications and merged portions thereof in any form. It will also terminate upon the conditions set forth elsewhere in this Agreement or if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the Program and its associated documentation, together with all copies, modifications and merged portions thereof in any form.
- 8. GENERAL
  - a. You may not sublicense the Program or its associated documentation or assign or transfer this license. Any attempt to sublicense, assign or transfer any of the rights, duties or obligations hereunder shall be void.
  - b. This agreement shall be governed by the laws of the State of California.
  - c. Address all correspondence regarding this license to RSA's electronic mail address <rsaref-administrator@rsa.com>, or to

RSA Laboratories ATTN: RSAREF Administrator 10 Twin Dolphin Drive Redwood City, CA 94065 USA

d. TO RECEIVE THE PROGRAM AND ITS ASSOCIATED DOCUMENTATION BY ELECTRONIC TRANSMISSION, YOU MUST TRANSMIT THE FOLLOWING ACCEPTANCE AND ACKNOWLEDGMENT TO RSA'S ELECTRONIC MAIL ADDRESS <rsaref-administrator@rsa.com>:

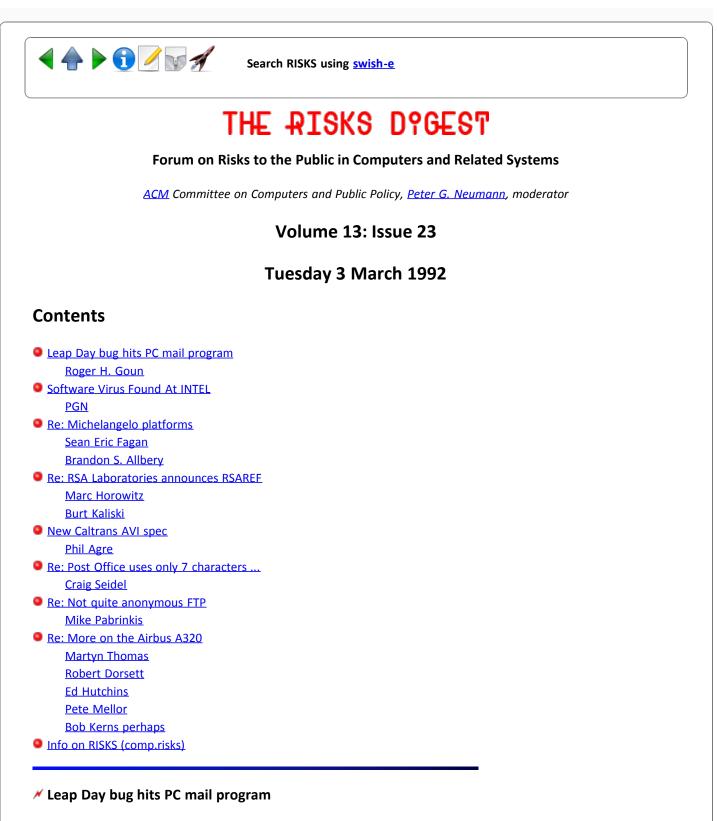
#### ACKNOWLEDGMENT AND ACCEPTANCE

I acknowledge that I have read the RSAREF Program License Agreement and understand and agree to be bound by its terms and conditions, including without limitation its restrictions on foreign reshipment of the Program and information related to the Program. The electronic mail address to which I am requesting that the program be transmitted is located in the United States of America and I am a United States citizen or a permanent resident of the United States. The RSAREF License Agreement is the complete and exclusive agreement between RSA Laboratories and me relating to the Program, and supersedes any proposal or prior agreement, oral or written, and any other communications between RSA Laboratories and me relating to the Program.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Roger H. Goun 03-Mar-1992 1243 <goun@ddif.enet.dec.com> Tue, 3 Mar 92 09:44:48 PST

UUPC/extended is a mail system for personal computers running MS-DOS. (The name is a pun on UUCP.) On Leap Day, Saturday, 29 February 1992, UUPC's UUPOLL program, which polls a remote system for mail at regular intervals, consistently hung the PC on which it was running. One workaround was to set the system clock ahead a day to 1 March.

Drew Derbyshire, the author of UUPC, traced the problem to a bug in the mktime() library function in Borland C++ 2.0, which converts a time to calendar format. Drew demonstrated that mktime() will hang a PC on Leap Day, and reported the problem to Borland. As distributed, UUPC is compiled with Borland C++ 2.0, though source code is available for do-it-yourselfers. Apparently, Borland has issued a corrected version of the library function (I haven't verified this).

Drew tried to warn UUPC users by mail after discovering the problem on Saturday. Ironically, many did not get the message until Sunday or Monday, when they found their PCs hung in UUPOLL.

Roger H. Goun, Digital Equipment Corporation, goun@ddif.enet.dec.com or goun%ddif.enet@decwrl.dec.com, {pacbell,pyramid,uunet}!decwrl!ddif.enet!goun

### Software Virus Found At INTEL

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 3 Mar 92 9:39:50 PST

From the N.Y. Times News Service, 3 March 1992 (I saw it in the SanFranChron):

Intel Corp. said Monday it had stopped shipping a computer network software program because some units were found to be infected with the ``Michelangelo" virus, a program that infects IBM and compatible personal computers and can potentially destroy data.

A division of Intel in Hillsboro, Ore., said it had shipped more than 800 copies of the program, called LANSpool 3.01, which inadvertently contained the virus. The virus is designed to activate on March 6, Michelangelo's birthday, and can erase data and programs if it is not detected with antiviral software.

The company said it had checked its software with a virus-scanning program before shipping it, but that it had failed to detect the virus.

A number of computer makers and software publishers have issued similar alerts about the Michelangelo program and a variety of companies are now offering free software to check for the virus.

There are more than 1,000 known software viruses that can copy themselves from computer to computer by attaching to programs and files.

### Ke: Michelangelo platforms (Bontchev, <u>RISKS-13.22</u>)

Sean Eric Fagan <sef@kithrup.com> Tue, 3 Mar 92 15:31:43 PST

>Sigh... Sorry, but this is FALSE! The Michelangelo virus attacks any IBM PC>compatible computers. There is no need that they are MS-DOS machines. You can>get a 80386 and install only Xenix on it, without any MS-DOS partitions.

That's a pretty amazing feat, since to do this, it would have to a) be a UNIX (or XENIX) binary, not a DOS binary, b) somehow get root access on the machine, c) figure out which device is actually the disk, and then d) munge it (d is, of course, the easiest part). Even if you run it under a DOS emulator, it is usually configured such that a DOS program cannot access any random device, or open up a disk drive (e.g.., it provides a pseudo-disk, for programs that like to just open up the disk under DOS themselves... but it cannot open up, say, /dev/root unless /dev/root available via normal permissions to the person who started the program).

I think you are seriously confused about things, and I will continue to believe that until I see proof otherwise.

Sean Eric Fagan

# Ke: Michelangelo platforms (Bontchev, <u>RISKS-13.22</u>)

Brandon S. Allbery KF8NH <allbery@ncoast.org> Tue, 3 Mar 92 19:25:05 -0500

Sigh... Sorry, but this is FALSE! The Michelangelo virus attacks any IBM PCcompatible computers. There is no need that they are MS-DOS machines. You can

Incorrect. The virus CAN affect machines that run Xenix or UNIX, but ONLY if they are booted from MS-DOS with an infected floppy disk. UNIX filesystem and program mechanisms, even on UNIXes that support "mounting" of MS-DOS floppies, will not permit the Michaelangelo virus to install itself under UNIX or Xenix. The worst that can possibly happen is that a VP/ix or DOS-Merge partition will be infected, but \*if it is only used under VP/ix or DOS-Merge then the primary boot track will not be affected because VP/ix and DOS-Merge will not allow it to be accessed\*.

Misinformation about viruses is yet another RISK that must be considered. I've encountered an article on Usenet from someone who thought (erroneously) that ALL computers would be affected (perhaps due to the events detailed in the original RISKS submission?). This further claim that the virus can somehow install itself on computers that are never booted into MS-DOS is just as incorrect.

Brandon S. Allbery, KF8NH [44.70.4.88] allbery@NCoast.ORG Senior Programmer, Telotech, Inc. (if I may call myself that...)

# Ke: RSA Laboratories announces RSAREF free cryptographic toolkit

Marc Horowitz <marc@MIT.EDU> Tue, 03 Mar 92 15:17:24 EST

Lawyerspeak from hell. Two questions:

<> b. The Program is to be used only in connection with a single computer.

Isn't this kind of stupid in the license of a program which is fundamentally most useful in a networking environment? Or, since licenses are free, should I get a few licenses for myself, in case I happen to want to run it on multiple machines? <> d. You may not translate the Program into any other computer language.

Including RTL, or assembler? Darn. Can't compile it, then.

RISKS of boilerplate legalese? Marc

#### KRSA Laboratories announces RSAREF free cryptographic toolkit

Burt Kaliski <burt@RSA.COM> Tue, 3 Mar 92 13:52:01 PST

Good points. We'd happy to receive comments on the legal agreement, since there aren't many things like RSAREF to compare against. We were aware of the "lawyerspeak" on the number of copies; it's pretty conventional, and we don't intend to keep anyone from storing more than one personal copy for personal in a network environment. But we wanted to start with conservative language. On the issue of translating into another language, your observation "Can't compile it" is a good one ... But of course you can compile it. Let's see if we can work out some better language.

I invite you to join the RSAREF user's group <rsaref-users@rsa.com>, which will discuss issues such as the license and help us improve things. To join, send email to <rsaref-users-request@rsa.com>.

-- Burt Kaliski, RSA Laboratories

## Mew Caltrans AVI spec (<u>RISKS-13.09</u>, <u>RISKS-13.13</u>)

Phil Agre <pagre@weber.UCSD.EDU> Tue, 3 Mar 92 13:00:37 -0800

Chris Hibbert (xanadu!hibbert@uunet.uu.net) is correct that I misinterpreted the AVI spec in one important way. The spec no longer calls for a VIN to be transmitted (the term VIN no longer appears in the spec) but rather the transponder's unique 32-bit code (see section 1705.5(e)(1). (I was misled by the retention of the term "AVI".) This is a significant improvement PROVIDED that transponder id's are not indexed against VIN's (or SSN's etc) when the transponders are sold or installed. The transponder is still to be fixed to the front bumper (1705.3, 1705.8), as opposed to being bought at 7-11 and kept in one's glove compartment. Whoever does the installing or collects payments will probably have enough information to register the transponder by VIN or license number. And this doesn't even count future uses of the transponders (e.g., 1702.1); future Transaction Record Formats could contain the VIN or just about anything else. Thus it is true that "The new draft doesn't leave room for an identifier of the vehicle or the driver in the communication packets", but it is also misleading.

I was unclear with regard to the issue of extensibility. Earlier versions did mention the possibility of extension, but the latest is much more explicit

on the subject. It is also more careful about separating out AVI-specific features from the underlying generic device.

A number of people have corresponded with me about how one might implement toll collection without requiring every car to carry a transponder. My real complaint had to do with the whole notion of a "spec". Chris says that "The spec doesn't talk about [the broader process of toll collection] because it's not part of the technology being designed." But this is only true on the narrowest possible definition of "the technology being designed". More socially relevant definitions are possible.

The folks proposing the Privacy Act reprinted in recent Risks issues are aware of these issues and seem sincere in their desire to protect privacy. But I am horrified by Chris' report that:

Some [Caltrans folks and vendors] are willing to say that they expect "other forces" (maybe DEA or INS?) to try to make this kind of equipment usable for tracing people's movements. There may have been attempts to make this be standard equipment on new cars.

The atrocious record of the DMV and the reputed attitude of Caltrans provide little comfort, and it would take a small twitch of California politics to put all the Senator Lockyers on the street in a few years. If personal tracking technologies cannot be made inherently resistant to civil liberties abuse then they should be banned.

Phil Agre, UCSD

## Ke: Post Office uses only 7 characters ... (Piatko, <u>RISKS-13.21</u>)

Craig Seidel <seidel@puma.sri.com> Tue, 3 Mar 92 13:50:12 PST

It sounds like you are the victim of two human errors and one piece of odd coincidence. First, your mail carrier incorrectly decided to place that mailpiece in a change-of-address bin. Then, the change-of-address mail was passed Computer Forwarding System (CFS) where the seven digits you described were typed in. By coincidence, there was someone on your carrier's route (or the wrong carrier route was typed in) with certain address similarities who had recently moved (I believe information is maintained for 1.5 years). Finally, the person who applies the yellow label is supposed to check the name and apparently didn't.

Seven digits are usually sufficient because mail typically doesn't get to the CFS unless the mail carrier is aware of an address change. Quality control at the final step was probably lacking for the typical reasons (working too fast, fatigue, boredom, etc.).

Craig

Ke: Not quite anonymous FTP (Rucklidge, <u>RISKS-13.21</u>)

<mpabrin@relay.nswc.navy.mil> Tue, 3 Mar 92 13:43:04 EST

> The risk is not so much that the logs are made, but more that the service> is presented as "anonymous", leading people to believe that it actually is.

By his tone and statements William Rucklidge shows himself knowledgeable about various logging techniques, both administrative and security-oriented, as found on many networked hosts, So, what bothers me? Two things...

First: Network application protocols have evolved over 15 years and more. FTP has ALWAYS been a man-in-the-loop protocol. The FTP-user must use a (different on each, we pray) valid ID/PW combination on each of the SOURCE and TARGET hosts; i.e., must be able to log on or in to each host to migrate any file from SOURCE to TARGET. Various host administrations realized it would be of value for a given SOURCE host to make certain files/directories widely available, without having to register huge numbers of users. Result: ANONYMOUS FTP, in which the valid ID/PW combination on the SOURCE host only, and for a limited file or directory set, reduces to an advertised pair such as "anonymous" and "guest", or "anonymous" and "any-non-null-string", etc.

The meaning of 'anonymous' here is NOT that no one logs such a transaction; rather, that the user can obtain files without being a registered user of the SOURCE host. 'Anonymous' here equates to convenient, not unidentifiable.

Second: William Rucklidge implies, maybe even states, that a widely-known Internet host permitted itself to be an anonymous FTP TARGET. I hope not!

However, even if the MBDF-A virus was migrated TO a TARGET host by someone using a registered ID/PW combination, that indicates a breakdown of trust at some point. Perhaps the (SOURCE or) TARGET host administrator did not know his user. Perhaps the user shared his ID/PW combination. Perhaps someone or two stole an ID/PW combo. I don't know, and my speculations are ignorant and dangerous. My point: host and network use is built upon and dependent upon trust. Trust is a fragile thing, the substrate of cooperation.

William Rucklidge, writing from a host apparently at the site where the two people alleged to have spread the virus were arrested, seems to imply that 'anonymous' ought to mean unidentifiable. I hope I misinterpreted what he wrote. In any society built and dependent on trust, such as our Internet, a user should NOT want anonymity, not even as a matter of FTP convenience; surely, NEVER as a mechanism for evasion.

Mike Pabrinkis, Naval Surface Warfare Center, Dahlgren, VA 22448 (703)663-7743 (AV)249-7743 <mpabrin@relay.nswc.navy.mil>

## Ke: More on the Airbus A320 (<u>RISKS-13.21</u>)

Martyn Thomas <mct@praxis.co.uk> Fri, 28 Feb 92 17:34:27 GMT

If the rate of descent was really 3,300 feet per minute, as reports suggest,

then 200 ft gives 3.636 seconds before impact, assuming flat terrain. I do not have information about the terrain. Allowing two seconds to react, is this enough time to go around? I believe that go-arounds can be executed from a few feet, \*if they are expected\*, and if the engines have not spooled down. I wonder what the tolerance on the 200 feet is, and what the allowable delay in generating the message is? The slant angle of the beam will affect the actual height at which 200 ft is measured, unless this is corrected for.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

## Ke: More on the Airbus A320 (<u>RISKS-13.19</u>)

Robert Dorsett <rdd@cactus.org> Fri, 28 Feb 92 13:43:58 CST

It's wrong to assume this is really a crash-alert system, like a GPWS. It's designed for use with an airliner flying a normal approach. Confused? Allow me explain!

In a normal airplane, duties are divided between pilot flying and pilot-notflying. Pilot flying flies the approach: manipulates the control column, throttle, autopilot, etc. Pilot not flying handles radios, checklists, navigation, systems, etc. During the last few minutes of the approach, he makes call-outs: decision height (when one has to go around if the runway's not in sight), and a variety of standard altitudes (1000', 500', 200', 100', 50', etc). All "above ground," as opposed to regular altimeter readouts, which are usually "above mean sea level." (exception being the radio altimeter, which always displays distance above the ground immediately underneath the sensor). I can really digress on this point, if pressured. :-)

The call-out practice is intended to enhance the situational awareness of the pilot flying the airplane, as well as the crew as a whole. The exact call-outs are normally subject to airline policy and the approach being flown: some are very superficial, while others have call-outs at practically every 20 feet.

During these call-outs, it is assumed the airplane would be in the "safe" GPWS envelope, since it's flying a normal flight path, presumably over level terrain at this point, and bumping into a sloping mountain isn't much of an issue. GPWS doesn't know the difference between an airport boundary and a cornfield, and it would be irritating to have a major warning every time the airplane simply passes a threshold altitude.

On the A320, of COURSE, the call-outs are automated, freeing the F/O to do other things. The system makes all call-outs, including one just before touchdown, reminding the pilots to activate the thrust reversers, by yelling "RETARD!" You can bet this improves the self-esteem of the pilots. :-)

So, again, this is all pretty irrelevant to the Strasbourg crash. The system isn't a warning or caution; it's just advisory. Whether we want the system to be \*automated\* is another question entirely, though. As stated, the practice is designed to improve crew communication. The whole idea behind call-outs is to verify that pilot A flying the airplane is thinking the same thing as pilot B, who is making the call-outs. All automated call-outs accomplish is to verify that Pilots A & B both \*independently\* agree that the computer knows what it's doing; they may then grow to rely upon its accuracy, and on the other pilot to cross-check his own instruments. Automated call-outs are yet another interesting new dimension on the functional social atmosphere and professionalism of the cockpit environment.

Another practical consideration is that, considering the human factors problems of tape-style instruments, which provide the altitude and airspeed indications on the A320, I think it would be a good idea to keep the PNF calling out the altitudes, rather than rely on the radio altimeter computer. Especially when one considers all the approaches that DON'T have a nice, smooth field for miles around the airport, but rather are on mountains, near cliffs, etc., and will cause the radio altimeter to think it's much higher than it actually is. A human pilot could cross-check with the barometric altimeter; the computer is designed to work with the radio altimeter.

As for the three seconds they may have had on the Air Inter, and what they might have done with them: who knows? If they were in a cloud, they'd be inclined to believe their instruments and continue flying the airplane, checking secondary sources for confirmatory information. And there goes the three seconds. On an airplane which is prone to spurious warnings, they'd probably ignore it, especially if they think they're at 8,000', 3000' above their target altitude, which, in turn, is a couple thousand feet above the maximum terrain elevation for the sector. And then there's the good possibility they had much less than three seconds, since, even though they were descending at 3000 fpm, they were also going forward at 180 knots or so. Pete's comment of 1 second tends to support this idea.

As an aside, good pilots do not yank back on the controls and perform dramatic maneuvers every time a light goes off: more accidents have been caused by that sort of behavior than otherwise. There's an old story of an astronaut -- Gus Grissom, I believe -- who was suddenly presented with a rather dramatic array of warnings while on the pad. Rather than start flipping switches instantly, as training required, he took a second or two to get his bearings, and study the situation. In that period, the systems reset, and the warning lights went out. He's commented that if he HAD started doing things instinctively, he could have REALLY got himself into a lot of trouble.

I suppose there's a moral there for systems that perform automated tasks on the basis of immediate data--and don't give the pilot the final authority to correct those mistakes, when spurious data corrects itself or is identified. GIGO rules.

Just my \$0.02.

Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd

# More on the Airbus A320 (Dorsett, <u>RISKS-13.22</u>)

Ed Hutchins <hutchins@cogsci.UCSD.EDU>

#### Fri, 28 Feb 92 18:05:49 PST

Just a comment on the function of callouts. In any airplane, automated or not, callouts on the final approach do more than ensure that both crew members share a notion of what is going on. Flying an approach is a visually intensive task for the pilot flying regardless of the weather conditions. An auditory callout by the PNF provides the pilot flying with important information in a sense modality that is not already heavily loaded. United Airlines, for example, mandates a callout at 500' above touchdown that includes the radio altitude, the descent rate, and an indication of speed relative to the target approach speed. For example, "five hundred feet, seven down, plus four" would mean seven hundred feet per minute descent rate, and four knots above target approach speed. When you are trying to pick up the approach lights in broken clouds and would like to transition from instruments to outside references, it is real nice to learn (without having to look) that you are on path, with an appropriate descent rate and a have few knots of speed over the target.

If any of you find that the first recommendation of the commission report translated by Peter Mellor smells suspiciously like a commitment to a cause for this accident, you might be interested to know that Northwest Airlines began a program to develop new crew procedures for the use of flight path angle and vertical speed modes in their A320's before the latest accident happened. I think the problems have been known to airlines operating the A320 for some time. Even if it turns out that the accident was not caused by a confusion of these modes, the report acknowledges that it is an issue that ought to be addressed.

Edwin Hutchins, Department of Cognitive Science, U.C. San Diego La Jolla, CA 92093-0515 ehutchin@ucsd.edu

## Ke: More on the Airbus A320 (Thomas on <u>RISKS-13.21</u>)

Pete Mellor <pm@cs.city.ac.uk> Fri, 28 Feb 92 19:04:24 GMT

The following is a translation of the relevant paragraphs of the interim report:

The point of impact was situated at an altitude of around 800 metres on the south-west slope of "la Bloss" mountain, which rises to 823m (see map in annex 1). At this place, the ground slopes upwards. The amount of slope varies between 8 and 17%. A forest of pines about 25 metres tall covers the entire area. The distance over which trees had been damaged was about 120 metres.

Measurements taken of the damaged trees allowed a rough estimate that the aircraft entered the trees at an angle of descent of about 12 degrees, with a roll inclination of the order of 18 degrees.

---End of extract

The map in annex 1 is large scale, and shows very little.

Obviously "slopes upwards" means upwards in the direction in which the aircraft was travelling.

The flight data from the QAR approximately confirms the above estimates. The QAR was burned, and in particular the last 25 seconds worth of tape prior to impact was damaged, and had to be read by special means. The last frame that has been read so far is at impact -4 seconds. This final reading shows:

Barometric altitude = 2750 ft Radio altitude = 600 ft Vertical speed = -4000 ft/min (and seems to have been increasing) Airspeed = 186 kt Bearing (cap) = 68 deg

To calculate time to impact from the point at which the radiosonde reported 200ft (which it would have measured relative to the tree-tops), we must take into account the upward slope of the ground, as well as the horizontal and vertical speeds of the aircraft. The airspeed would need to be corrected for wind velocity to get ground speed. The meteorological report for the area of the crash site gives wind between 1000 and 2000 metres as north-east or east-north-east 25 to 35 kt irregular, gusting to 40 kt.

Since it is nearly 7 pm, and I have a pint waiting for me in the Sekforde Arms, I will leave this calculation to somebody more dedicated, but bear in mind that the ground was uneven, so that any estimate is bound to be rough.

My own finger-in-the-air guess at the time to impact is "not very long". After they heard that "Two hundred feet" announcement, the pilots wouldn't even have had time to say "Merde!", never mind do a go-around.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V OHB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

# Ke: More on the Airbus A320 (Dorsett, <u>RISKS-13.20</u>)

<rwk@crl.dec.com> Sat, 29 Feb 92 07:31:44 -0500

Robert Dorsett writes:

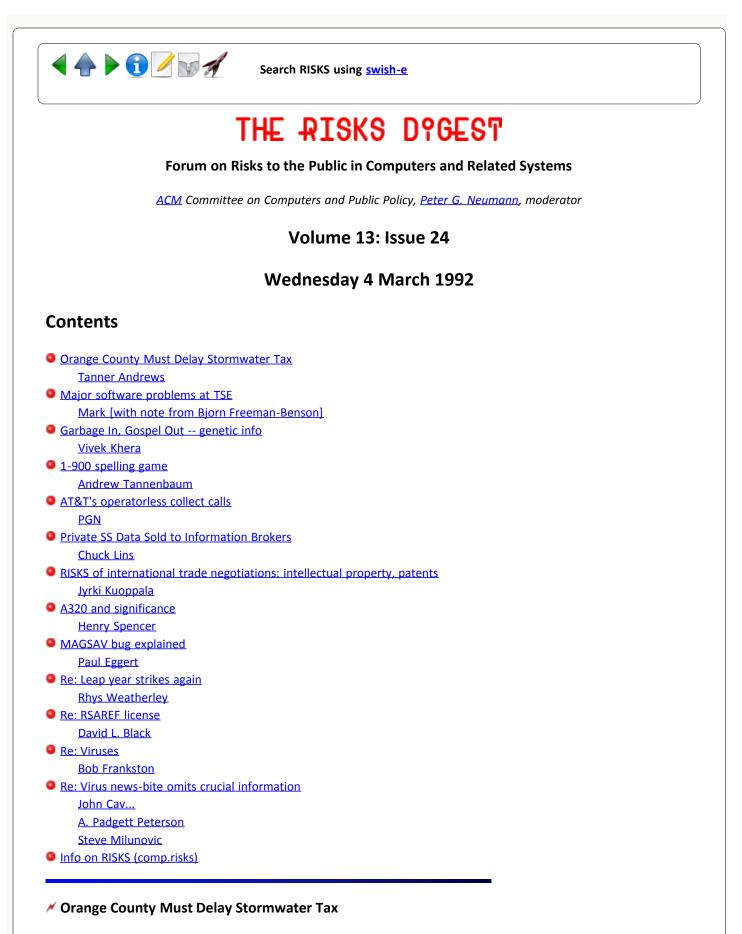
As with most crashes, the Air Inter crash was likely the result of a complex number of factors; no single protection could have "saved" the airplane.

I think you mean to say that any one of a number of factors WOULD have saved the airplane. It's the COMBINATION of the factors that caused the crash.

I certainly don't want to fly on anything so screwed up that it's going to crash for a whole bunch of reasons!



Report problems with the web pages to the maintainer



Dr. Tanner Andrews <tanner@ki4pv.compu.com> Tue, 3 Mar 92 7:26:02 EST The \_Orlando Sentinel\_ [remarkably acerbic comments about the paper have been deleted by your immoderator] cost Orange County a year's delay in passing a stormwater tax. They failed to run two of the required advertisements for a public hearing.

Yeah, ``it's the computer's fault."

...!{bikini.cis.ufl.edu allegra uunet!cdin-1}!ki4pv!tanner

### Major software problems at TSE

<mark@orca.cita.utoronto.ca> Wed, 4 Mar 92 05:24:05 EST

> TSE computers go berserk, floor closed for four hours Breakdown bolsters opposition to computerized trading BY CAROLYN LEITCH, Toronto Globe and Mail, 4 March 1992, business section, lead item

A software glitch caused computers at the Toronto Stock Exchange to go berserk yesterday, scrambling information, recording wildly inaccurate prices and failing to print tickets to confirm trades. Floor traders quickly used the breakdown to bolster their opposition to the TSE's planned move next year to an entirely computerized trading floor. The malfunction also illustrated the problems many organizations encounter when they try to change the software code that instructs computers.

TSE officials closed down floor trading for nearly four hours between 10 a.m and 2 p.m. after irregularities were detected in the computer system that traders use to buy and sell equities. Carl Christie, a senior professional trader with Nesbitt Thomson Deacon Inc. and chairman of the Professional Traders Association, said he noticed dramatic problems shortly after the market opened at 9:30 a.m. An order to buy 20,000 shares in Teck Corp. at \$17.37 a share appeared on the computer as a bid for 3,339 shares at \$279.50 a share, he said. As well, some sellers were unaware their sell offers had been accepted because the system was not printing confirmation tickets.

The TSE said it didn't know if it would have to unwind any of the trades. The exchange said disputes over orders that went awry will be decided on a case-by-case basis by floor governors. Mr. Christie said that as as specialized trader with certain stocks, he had no flow of orders coming in during yesterday's shutdown. As many as 150 other traders were also affected, he added. "I know that it cost me money -- we lost two-thirds of our working day."

The TSE has voted to replace floor trading with a fully computerized system early in 1993. That decision is unpopular with floor traders who fear for their jobs.

The bugs appeared after the TSE changed its computer software over the weekend to deal with new trading rules. Olaf Kraulis, vice-president of information systems at the TSE, said the system was restored to its pre-weekend

state after flour hours of grappling with the problem. He said the software changes will be reinstated in one or two weeks after programmers figure out why they fouled up the computer system.

But Don Unruh, a former TSE vice-president who helped develop the system eight years ago, said the problems run deeper than yesterday's malfunction. A patchwork of different software and hardware has emerged over the years, he said. "The people who are making the changes eight years later have no idea what was done by the people who went before them. You end up with these bizarre logic problems." Mr. Unruh, now a consultant who recently wrote a report on the TSE's computers for the Professional Traders Association, said the whole system should be scrapped and a new one developed.

But Mr. Kraulis said thousands of changes are made to software every year with few problems. While the 12 Tandem Computer processors that power the system have backup provisions in case of a hardware failure, there is no such contingency for software problems. "If a copy of the software is wrong, every copy will be wrong," he said.

Leonard Petrillo, the TSE's vice-president of corporate affairs, said the impact on members was minimal. "Most of the stocks are inter-listed," Mr. Petrillo said, "and traders were able to instantaneously reroute orders to other exchanges," such as the Montreal Exchange and the New York Stock Exchange. [...]

[Also submitted by bnfb@csr.UVic.CA (Bjorn Freeman-Benson), who added this:]

[The RISKS? Besides the obvious ones, the interlisting could motivate traders to avoid an unreliable Toronto in favor of Montreal, which is a risk to the computer owners rather than the computer users... Bjorn]

[How about the risk of sabotage by dissident floor traders? PGN]

### ✓ Garbage In, Gospel Out -- genetic info

Vivek Khera <khera@cs.duke.edu> Wed, 04 Mar 92 13:39:16 EST

Summarized from the March 2, 1992, Newsweek, page 58: "Eve Takes Another Fall"

In 1987, a group at UC Berkeley used a computer to analyze mitochondrial DNA from 147 people and proclaimed that all humankind descended from one woman who lived in Africa 200,000 years ago. Last year the team ran a more rigorous analysis using 189 samples and again concluded the same thing.

The program tries to find the family tree that is most "parsimonious"; that is, a tree based on the fewest genetic mutations. The trouble is that there are multiple equally parsimonious trees, and no algorithm to guarantee the computer has found the best one. The resulting tree depends on the order of the data input. The Berkeley group assumed the order of data was irrelevant. "They weren't using the program in an adequate way," says Alan Templeton of

#### Washington University.

One explanation of why it took so long to discover this error: ``...[they] didn't have the mathematical savvy to understand the statistical traps in the computer."

ν.

[... cloning primordial parsnips in a pearsimonious tree? PGN]

### 1-900 spelling game

Andrew Tannenbaum <trb@ima.isc.com> Wed, 4 Mar 92 14:38:50 -0500

There is an ad on TV for a 1-900 telephone service spelling game - if you can spell twenty words correctly in two minutes, you win \$200. I guess you hear the words and type them in on your touchtone pad. Assuming that the game isn't rigged to make it impossible to win, it would be pretty easy to devise a hack to allow you to type words on your PC, check their spellings, and send out the correct touch-tone signals on the fly.

The parts for this hack are readily available. There are good spell checkers and big dictionaries (word lists). Modems these days have dialers that generate touch-tone, it ought to be possible to program them to talk to the spelling game (sending tones at the proper speed and spacing). I imagine that this computer-aided approach would improve your odds to a significant extent.

Andrew Tannenbaum Interactive Cambridge, MA +1 617 661 7474

### AT&T's operatorless collect calls

"Peter G. Neumann" <neumann@csl.sri.com> Wed, 4 Mar 92 18:33:33 PST

Andrew's message reminds me of this morning's news item that AT&T will need far fewer operators because it is automating voice processing to eliminate some operator assistance. (The scheme is already being tested in various areas.) The collect call initiation permits the caller to pack an arbitrary short message into the time slot for the caller's presumed name. I imagine that will open up all sorts of new games that are currently prevented by operator assistance. On the other hand, it has always been possible to do that now with a little prearranged coding. With the new scheme, you would not even have to resort to Tuesday Weld to anticipate arrival in Maine, Gal Friday to indicate Galveston, etc.) It would seem to be much more flagrant with the new scheme. So, maybe they will try to filter out strange sequences. Blocking short bursts of 2.4Kb data transmissions might be possible, for example! But it would be terrible to restrict it to small dictionaries like telephone book names suitably pronounced without too much of an accent. This sounds like a freebie fraught with fraud, I'm afraid.

## Private SS Data Sold to Information Brokers

"Chuck Lins" <chuck\_lins2@gateway.qm.apple.com> 4 Mar 92 08:12:32 U

Private SS Data Sold to Information Brokers San Jose Mercury News, Saturday February 29, 1992.

Private Social Security data sold to 'information brokers' By R.A. Zaldivar, Mercury News Washington Bureau

Washington - The privacy of 200 million Americans with records at the Social Security Administration is threatened by an illegal trade in pilfered computer files. Computerization has dramatically improved our ability to serve the public," Social Security Deputy Commissioner Louis Enoff told a Senate panel Friday. "However, it has also made confidentiality more difficult."

Two executives of Nationwide Electronic Tracking, a Tampa, Fla., company, pleaded guilty to conspiracy charges in January for their part in a national network selling Social Security records. Twenty-three people, including agency employees and police officials, have been indicted in the case - the largest known theft of government computer data. "Information brokers" will pay Social Security employees \$25 for a person's earnings history and then sell the data for as much as \$300. Their growing list of customers includes lawyers, private investigators, employers, and insurance companies.

Social Security records contain a mother lode of information that includes not only a person's past earnings but names of employers, family history and even bank account numbers of people who receive benefits by direct deposit. The information can be used to find people or to make decisions on hiring, firing, suing or lending, said Larry Morey, deputy inspector general of the Health and Human Services Department.

"Here we have a large-scale invasion of the Social Security system's confidentiality," said Sen. Daniel P. Moynihan, D-N.Y., chairman of the Social Security subcommittee.

Information from other government data bases with records on individuals - such as the FBI's National Criminal Information Center - is also available on the underground market. All a broker needs is the cooperation of a clerk at a computer terminal.

Congress may revise privacy laws to increase penalties for illegally disclosing information in the private files of individuals.

Enoff said Social Security is studying ways to improve computer security, as well as keeping closer tabs on employees with access to files, and stressing to its workers that unauthorized disclosure of information is a federal crime.

Perhaps if release of information was keyed to a digital signature of the [clerk, this could be used to identify those persons (at SSA) selling the information. No mention is made of the buyers of the information from the

broker. I guess they just get to keep the illegally obtained information.

Now I wonder what happens when this happens in California at the DMV, and a copy of my digitized signature is sold? Chuck Lins lins@apple.com]

### KISKS of international trade negotiations: intellectual property, patents

Jyrki Kuoppala <jkp@cs.hut.fi> Wed, 4 Mar 1992 17:59:38 +0200

There has been an attempt in the UN organisation World Intellectual Property Organization, WIPO, to harmonize world's patent laws. It seems to be that USA is just about the only country who is pressing for "patents on all fields of technology" while many countries oppose things like patents on software and biotechnology. The developing countries say that many patents are one of the Western worlds' ways of keeping ahead in the game and keeping the developing countries behind.

In UN, it's one vote per country so USA has not been very successful. However, USA seems to have more success via GATT, as Kurt Jaeger writes on misc.int-property:

"Look e.g. on rusmv1.rus.uni-stuttgart.de [129.69.1.12] in directory info/comp.patents/lpf-de/docs/GATT-draft.txt.Z, its a copy of the TRIPS stuff in the GATT treaty (TRIPS == trade <something> intellectual property

# A320 and significance (Ilieve, <u>RISKS-13.21</u>)

<henry@zoo.toronto.edu> Wed, 4 Mar 92 18:33:23 EST

>Unless you assume that the pilots flying A320s are more stupid than >average, then if pilots have more crashes in A320s than other planes, >even if the cause is officially `pilot error', there must be something >about the plane that makes errors more likely.

My statistics friends would laugh at this, or sigh and shake their heads. The proper version is "...if pilots have \*significantly\* more crashes...".

One must remember that COINCIDENCES DO HAPPEN. Remember the time some years ago when it seemed that whenever you turned on the radio, there was another report of a DC-10 crash? Haven't heard many lately, have you? What changed? Basically, nothing. Oh, some minor changes were made in the aircraft and its operating procedures, but that spate of crashes was mostly sheer bad luck. Modern airliners very seldom crash; the DC-10 just had a couple of bad years, with mechanical flaws, bad maintenance, navigation problems, and (yes) pilot error all striking down the same type of aircraft at around the same time.

It's still actually open to doubt whether the DC-10 is significantly less safe than its competitors. The numbers do suggest so, but they are based on so few incidents -- compared to the enormous number of successful and

uneventful flights -- that it is entirely possible that the DC-10 has simply had bad luck. In military flying, with much higher accident rates, it is not at all uncommon for the investigation of a series of accidents to find that the failures were unrelated and the timing just coincidence.

On the whole, I think there is some reason to suspect that the A320 has human-interface problems. But that conclusion is based on the \*details\* of the cases so far, not on just counting them. It will be quite a while before we have enough data on A320 crash rates to start to draw any valid numeric conclusions about whether it really crashes unusually often.

Henry Spencer at U of Toronto Zoology utzoo!henry

#### MAGSAV bug explained

Paul Eggert <eggert@twinsun.com> Tue, 3 Mar 92 18:27:55 PST

G M Lack reports in comp.sys.prime <9203021236.AA01979@uk0x06.ggr.gri.com> that MAGSAV probably failed on 29 Feb 1992 because it tried to increment the year by one to set a tape label expiration date, and the resulting nonexistent date 29 Feb 1993 threw it for a loop. Alas, dates are tricky, and that goes double for date arithmetic.

### 🗡 Re: Leap year strikes again

Rhys Weatherley <rhys@cs.uq.oz.au> 4 Mar 92 03:23:50 GMT

I too experienced strange behaviour with Feb 29 dates. A Windows 3.0 newsreader I have been prototyping using Borland C++ 2.0 has been happily chugging along for a number of weeks without hassle. Then (of course) it locked up for no apparent reason.

Tracing the program revealed that during the parsing of "Date:" headers, when it called the "mktime" function to convert the dates to the Unix date/time format, it locked up. I haven't delved deeply into disassembling the code for "mktime", so I don't know the exact cause of the problem, but the call was very quickly replaced with an alternative version of "mktime". :-)

So, some of these problems; at least on PC architectures; may be attributable to bugs in the run-time libraries of Borland C++ and possibly Turbo C++ also, rather than to the authors of packages that use the run-time libraries.

Rhys Weatherley, The University of Queensland, Australia rhys@cs.uq.oz.au

### Re: RSAREF license

<dlb@osf.org>

## Wed, 4 Mar 92 14:36:09 GMT-0400

Shortly after this electronic license agreement showed up inside OSF, we received a missive from our attorney asking in no uncertain terms that we not execute the license (and revoke it and dispose of the software if we had). The major problem revolves around the fact that the technology is export controlled. The original posting stated:

- > 4. You can't send RSAREF outside the United States, or give it
- > to anyone who is not a United States citizen and doesn't
- > have a "green card." (These are U.S. State and Commerce
- > Department requirements, because RSA and DES are
- > export-controlled technologies.)

The problem is that the intuitive meaning of this paragraph is misleading. The intuitive meaning is that you must not intentionally do something that explicitly transfers the software to someone who should not have it (for brevity, call this individual a `restricted person'). Unfortunately, the actual restriction includes unintentional acts, and acts of omission (didn't do something you should have). An example could be include putting the source files on a system to which a restricted person has access (unbeknownst to you).

If something goes wrong, the government may come after both you and your employer (by holding your employer responsible for your actions). At the very least, anyone contemplating putting this software on one of their employer's systems should run the license past the appropriate lawyer. There are other more mundane reasons for a lawyer to say no, such as needing to formally verify that RSA really is who they say they are.

The RISK here is that the quasi-public distribution mechanism being set up by RSA may well be inappropriate for export controlled software. This is not like the copyright laws; people go to jail for violating export control laws.

Disclaimer I: This post is a statement about the export control laws; it has nothing to do with my views about how distribution of this software should (or should not be) controlled. If you've ever wondered about the restrictions that export control laws place on information interchange and technology transfer, you now have a concrete example.

Disclaimer II: Nothing in this post should be relied on as legal advice. If you think you might have a problem, go find a real lawyer.

--David L. Black (dlb@osf.org)

# 🗡 ... viruses

<Bob\_Frankston@frankston.std.com> Tue 3 Mar 1992 21:34 -0500

It is not public, but at least one large software company does put in some integrity checks in its software. While this isn't Virus protection, it is a step in the right direction.

I wonder if a more technical term like "Transportable Boot Sector Modification Programs" would engender the same amount of popular press. Question: How many people are going to start wearing gloves when they use their computers?

It is also interesting that an MSDOS Virus is getting this attention. Macs are actually more vulnerable since the passive insertion of a disk will cause the execution of a procedure whereas you must execute off the disk in order to run program on it. I presume that the larger number of PC users and, perhaps, more of a history of exchanging programs contributes to the spread.

The infection is actually worse in object-oriented systems since objects are active elements (i.e., they come with methods and behaviors. One can argue that any object IS a kind of Virus that comes with its executable code and relies on the local environment to give it life. Dealing with issues like this is what delays seemingly good ideas. In fact, over 25 years ago, there was to be T access in Multics. T stood for "Trap". When you attempted to access a segment with Trap access, a trap routine, provided by the segments owner would be run. Of course, it would have to be run in the owner's access domain with the user protected from bad behavior though the trap procedure would also be executing in some form of the user's environment. No surprise that T access didn't make into the (relatively) secure production system. But the thinking raise issues of mutually suspicious subsystems generating various theses. One indirect result is the ring architecture of the 386. The moderator and other readers can contribute many more details to this history.

By being naive, the Mac was able to implement a very user-friendly feature. A smart disk allows one to insert a disk and let it install itself. Only etiquette demands that it should ask permission before starting. The Mac also naively implemented bitmap fonts on a fixed size screen. Scaleable fonts weren't even imagined by most users.

So which is right -- the Multics approach of implementing a feature after it is somewhat understood or the Mac approach of doing what makes things easy for the user and then fixing it up later. Novell implemented a remote file system by patching into DOS in a way that 3com didn't. As a result, people bought Novell's product and Microsoft has to accommodate them. Cellular phones with their lack of security are another example. Conversely, all electronic devices brought onto airplanes are, for some reason, suspect. Apparently turning them on at a security point exorcises the daemons...

In the case of viruses, we might achieve a balance of terror by hanging a few creators (chosen by lottery) by their typing fingers and hoping the problem abates. Some firewalls will be added to software. The alternative of creating truly secure software is possible -- just prevent naive users from getting near computers.

#### Ke: Virus news-bite omits crucial information

<jcav@midway.uchicago.edu> Wed, 04 Mar 92 11:45:17 -0600 <> AT NO TIME DURING THE PIECE DID ANYONE MENTION THAT THE VIRUS <> AFFECTS MS-DOS CLONE MACHINES ONLY.

I wish to apologize for the extremely poor wording of my original article. The point I was trying to make was that the Michaelangelo virus does NOT attack Macintoshes, Amigas, SUN workstations, UNISYS mainframes, etc. etc., but the radio program made no mention of any such distinctions.

I used the phrase "MS-DOS clone machines" to mean IBM PC-compatible computers. I should have said that instead. Oh well.

#### JohnC

[There was a slew of messages on this subject, including those from Bennet\_Yee@PLAY.TRUST.CS.CMU.EDU, padgett@tccslr.dnet.mmc.com (A. Padgett Peterson), jct%se33@seg01.wg2.waii.com (Jim Thompson), tneff@bfmny0.bfm.com (Tom Neff), dholland@husc.harvard.edu (David Holland), and rslade@sfu.ca (Robert Slade).
I could not include them all, but there was lots of overlap. However, I pseudorandomly picked Padgett's, which follows. Read no further if you have had enough. And then wait for Friday. Thanks to all of you for rising to the occasion. PGN]

# Michelangelo & Unix Boxes

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Wed, 4 Mar 92 09:00:54 -0500

>That's a pretty amazing feat, since to do this, ...

Unfortunately, it is no problem at all since Michelangelo is a BIOS virus (no it doesn't infect the BIOS, it uses it) and this is present and essentially standardized (what makes a PC "100%" compatable) in every Intel box that is able to boot DOS.

The virus uses Intel iapx80x86 assembly language but only uses BIOS interrupts not MS-DOS interrupts (my FixMBR does also which is why it can repair "invalid" disks but needs DOS to load the program).

The important fact is that when a PC frst loads absolute sector 1 from a disk, it is already, courtesy of the BIOS, a fully functioning computer with the ability to address all of its peripherals. It is just not yet a MS-DOS (or PC-DOS, or OS/2, or Unix, or...) computer yet. The original Flight Simulator and many DOS 1.0 programs (the ones you had to boot from the floppy but were unreadable by DOS) were examples of BIOS-only programs.

Unfortunately, except for a few of us -and many virus-writers 8\*( -this seems to be a "lost art".

The problem that Michelangelo has stems from things it expects that are

characteristics of DOS and are not necessarily true:

1) That absolute sector 7 on the fixed disk is unused

2) That memory marked in software as "unavailable" by the BIOS will not be used

Neither assumption is necessarily true under Unix though it is usually (1) that causes Mich (or Stoned or ...) to fail on a Unix platform by making it unbootable.

BTW IMHO any damage that results from Michelangelo may be laid directly at the feet of the OS vendors for Intel based platforms (and this includes UNIX as well as DOS) who do nothing about "rogue programs" at the BIOS level (over 50% of all reported infections last year)

Ten bytes in IO.SYS (or the boot record, or the MBR like my stuff) are all that is necessary to find every MBR infector that I have come across including Brain, Yale, Aircop, Stoned, Evil Empire, Bloody, and many others including the Michelangelo.

The question is: if we do not take steps now to eliminate these viruses, what are we ever going to do about the really nasty and professional (the Michelangelo is very buggy & "crude") viruses that I know could be written ?

Padgett

# 🗡 Michelangelo

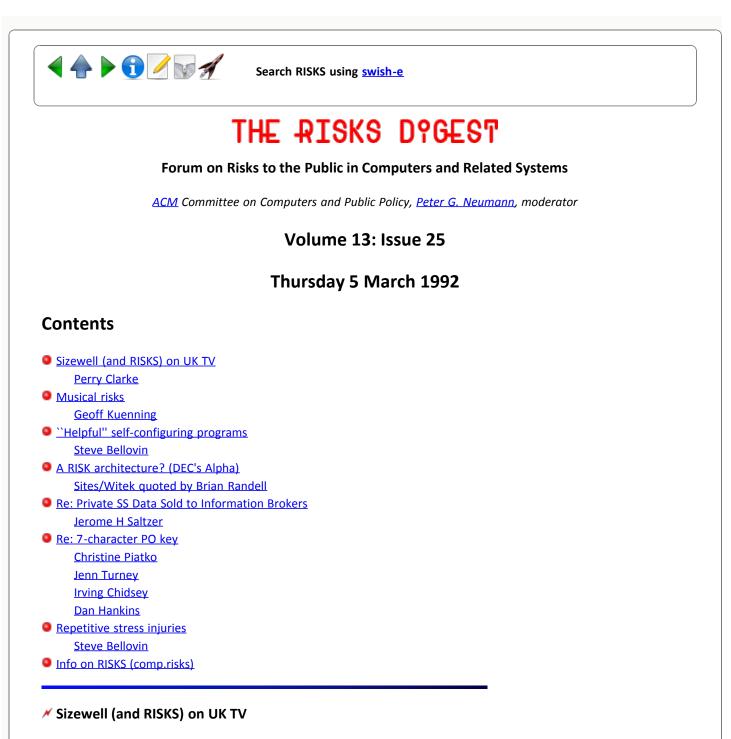
"Steve Milunovic" <steve\_milunovic@qm.sri.com> Wed, 4 Mar 92 9:55:36 PST

I wish there was some way to stop the media from spreading such bad advice as resetting the clock to circumvent the Michelangelo and other date virus strains. Don't they know the virus is still there and can become more widespread if it isn't removed? =Steve=



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Perry Clarke - Oracle Data Query Development - Chertsey" <dpclarke@uk.oracle.com> Thu, 5 Mar 92 13:18:06 GMT

On Wednesday, 04-MAR-92 Channel 4 TV in the UK broadcast a program concerning the difficulty of testing complex software systems - specifically the reactor shutdown system for the Sizewell B Pressurized Water Reactor that is currently under construction.

Nothing very new was said; it was the usual mix of nuclear industry suspicion of people's intentions when requesting information and people's concern with living in the same country as a nuclear power plant whose safety system cannot be properly tested. The angle that the program's producers had choosen to highlight was that it is software based and we have not figured out how to test (reliably) 100,000 lines of code.

The best bit was an implication that Nuclear Electric (the builders) had an inkling of the scale of the effort required to test the system properly and their attitude was that it would take so long and cost so much that it was obviously not practical :-)

In the course of the program we saw many screens purporting to show "computer programs"; a selection:

- o A .newsrc scrolling by (comp.risks makes a guest appearance!)
- o A UNIX directory listing
- o What looked like an abbreviated PostScript program

It seems that the risks associated with the untestability of complex software systems are beginning to be recognised by the layman. The message that the TV program gave me was of the concern of people outside the (software) industry that we do not know how to guarantee the reliability of our products.

The licensing of Software Engineers was not mentioned once.

UNIX Mail: dpclarke@uk.oracle.com (Soon to be: perry@unify.com)

## Musical risks

Geoff Kuenning <desint!geoff@uunet.UU.NET> Thu, 5 Mar 92 01:45:35 PST

The city of Los Angeles was recently graced with the world premiere of the new opera "Kullervo" by Aulis Sallinen, a talented Finnish composer. At the open dress rehearsal, I noted that the score seemed to include some synthesized sounds, which I later confirmed by an inspection of the orchestra pit. The synthesizer used was a Yamaha DX-7 II, which aficionados will recognize as an already-obsolete instrument which is no longer manufactured. I suspect that Mr. Sallinen (who appears to be in his 60's) is completely unaware that in twenty years it is going to be nearly impossible to acquire a working DX-7 to duplicate the sounds he intended. Perhaps synthesizer manufacturers will recognize this problem and include a backwards-compatibility mode, but more probably works written for live synthesizer performance (I seem to remember that "The Phantom of the Opera" uses a couple of synthesizers) are going to have to compromise on timbral quality.

It's already well-nigh impossible to duplicate the sounds of the old analog synthesizers with modern digital ones, but so far this problem hasn't affected mainstream classical music (rock and jazz have a double advantage, both because recordings dominate in listening to older works, and because flexibility in performance is not only accepted but expected).

This all gives a whole new meaning to the "original instruments" school of classical performance. I wonder if I could interest Christopher Hogwood in

building a collection of DX-7's? :-)

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

# \* ``helpful'' self-configuring programs

Steve Bellovin <smb@ulysses.att.com> Thu, 05 Mar 92 12:17:31 EST

On our Internet gateways, we run a variety of security monitors. Among other things, these detect attempts to connect to services that are generally of no legitimate interest to outsiders. But the alarm that went off the other day was a bit different; the services contacted weren't the usual targets.

The answer turned out to be fairly interesting. It seems that a university 5 timezones away was installing a new network management system. This program was, it seems, self-configuring -- it went out and tried to discover the topology of the network. The \*WHOLE\* network, as best I can tell.

I wonder how many sites were probed -- and didn't notice -- before I alerted the administrators.

There are all sorts of other implications, of course. For one thing, I don't know if I was being told the truth, though I have little reason to doubt it. And such a comprehensive network map can be used to commit all sorts of mischief. But as far as I know, that didn't happen this time. Steve Bellovin

## A RISK architecture? (DEC's Alpha)

<Brian.Randell@newcastle.ac.uk> Tue, 3 Mar 92 15:12:14 GMT

Quoting from: ALPHA ARCHITECTURE TECHNICAL SUMMARY (Dick Sites, Rich Witek) in comp.arch:

"Alpha is also unconventional in the approach to arithmetic traps. In contrast to conventional RISC architectures, Alpha arithmetic traps (overflow, underflow, etc.) are imprecise -- they can be delivered an arbitrary number of instructions after the instruction that triggered the trap, and traps from many different instructions can be reported at once. This makes implementations that use pipelining and multiple issue substantially easier to build."

... and to use safely?

However, the next paragraph does provide what I would classify as a sop to DEC's technical conscience by stating:

"If precise arithmetic exceptions are desired, trap barrier instructions can be explicitly inserted in the program to force traps to be delivered at specific points." Brian Randell, Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

### Ke: Private SS Data Sold to Information Brokers (<u>RISKS-13.24</u>)

Jerome H Saltzer <Saltzer@MIT.EDU> Thu, 05 Mar 92 14:18:39 EST

> "Information brokers" will pay Social Security employees \$25 for a> person's earnings history and then sell the data for as much as \$300.

In that case we had better on the watch for the enterprising congressperson who can do arithmetic and who notices that the SSA could go into the retail market itself, sell 200,000,000 records for \$60B, and close next year's budget gap.

The number seems high; one wonders whether \$300 is the market price for an SSA record selected at random, or for selected records in the Iacocca-and-above class.

Jerry Saltzer

## 7-character PO key (Piatko, <u>RISKS-13.21</u>)

Christine Piatko <piatko@cs.cornell.edu> Wed, 4 Mar 92 14:15:03 -0500

The ending of my last message should have read "it's \*not\* as much of a coincidence as you might think" -- here it is in it's corrected form:

I don't doubt that there were human errors as this particular piece of mail tried to make its way from the bank to my house. However, I think you are wrong about the seven characters being "one piece of odd coincidence." A significant fraction of Ithaca's population is made up of students (probably more than 1/4, but less than 1/2), and students move frequently. If you have a common last name it is pretty likely there's someone else with a similar last name who's also a student and lives in the neighborhood. And there are lots of street numbers in the 100 to 300 range in the areas where students live!

I looked at the student phone book and picked two common last names, Chen and Smith, and found 2 Chens that live at a house numbered 109 and two Smiths that live at a house numbered 210 in the Collegetown area. They all live on different streets and have different first names. I don't know if these particular examples would involve the same mail carrier, but I'm sure there are examples that do.

So it's not as much of a coincidence as you might think! That's why I think one or two more characters for the hash code would help.

Christine Piatko (piatko@cs.cornell.edu)

# // 7-character PO key (Piatko, <u>RISKS-13.21</u>; Seidel, <u>Risks-13.23</u>)

Jenn Turney <turney@cs.cornell.edu> Wed, 4 Mar 92 11:18:30 -0500

As the other person Christine mentioned who's had similar problems with mail forwarding in Ithaca, I have a hard time attributing the problem to "odd coincidence." I received occasional misforwarded mail (including, at one point, a COD delivery notice) over a period of about six months. As was the case with Richard Chang, the person's 7-letter key matched mine, but the names and addresses were clearly different. I would write "incorrectly forwarded" on the front of each and put them back in my mailbox. I sincerely hope they all eventually reached her; I never saw them again.

I had moved from Ithaca to Schenectady and back -- some of the mail forwarded made the round trip. Ever wondered whether "Return address requested" is attended to? The answer's yes -- I got a credit card bill with her name and my address on it! The last straw was an envelope from a local community college with my name and address handwritten on the outside and a loan form with her name and address on the inside. So not only did the postal employee not check that the names/addresses matched, but neither did the recipient of the forwarding information. The addition to the key of one letter from either the first name or the street name would have avoided the problem in my case and, by quick perusal of the phone book, several others.

Ithaca is a university town so naturally there are certain times when a large number of people move at once. This would seem to imply that it is especially important that we have a reasonable forwarding process. This one doesn't behave quite reasonably enough for me.

Jennifer (not Shelley) Turney (not ... well, you can guess)

## Ke: 7 characters (Piatko, <u>RISKS-13.21</u>)

Irving Chidsey <chidsey@smoke.brl.mil> 4 Mar 92 14:12:12 GMT

Now I know why the post office for greater metropolitan Selinsgrove, Pa. (all fits quite comfortably in one zip code) included one stray letter in my mother-in-law's forwarded mail when she stayed with us for a while last year. It may also explain why my income tax refund was returned to the IRS about five years ago. Still, considering how much mail is handled, and the large number of customers the post office serves, this seems to be a rare error. Much more common, in my experience, is getting mail intended for the family at the same street number, one street away, and I believe that is mostly 'operator error', because the letter carriers sort that themselves, by hand.

Irv

Ke: Post Office uses only 7 characters... (Seidel, <u>RISKS-13.22</u>)

<HANKINS@pkedvm8.vnet.ibm.com> Tue, 3 Mar 92 22:19:36 EST

Perhaps it's worth noting that this is one of those situations where adding redundancy to quality control -decreases- quality in what I like to call the "Kitty Genovese" effect.

I first noticed this in one of W. Edwards Deming's books. For each inspector one adds in series to a process, the greater the likelihood that a defect will go unnoticed. It works something like this:

With a single inspector, she knows that the next person to check the item she's inspecting is the customer. If something goes wrong, she is the one to take the blame.

With two inspectors, each relies on the other to inspect, so his inspection is somewhat less thorough. Also, if a defective unit gets through, the inspectors share the blame equally.

With 100 inspectors, almost no inspection at all is done; each thinks, "Surely with 99 other inspectors a defective unit will be caught!" As a result, all but the most glaring defects get through.

I counted three "inspections" in the mail handling process described; sorting by the mail carrier, typing in of the seven-digit code, and checking of the name by the person whose job it is to affix the yellow change-of-address stickers.

Dan Hankins

# Repetitive stress injuries

<smb@ulysses.att.com> Wed, 04 Mar 92 15:05:05 EST

By coincidence, the New York Times has just run a pair of articles on the subject of repetitive stress injuries. I've enclosed substantial extracts from the two articles. Speaking personally, I find that I have more trouble with my wrist when I'm very tired to start with. (I'm very tired right now, and I almost didn't prepare this message because my tendonitis is acting up again.) A wrist rest helps me immensely. Conversely, too much mouse activity is problematic, since I don't have effective support for my wrist then. Typing on too high a surface -- such as a regular desk, as opposed to a typing table -- is a sure-fire recipe for trouble (again, for me). It's even worse if the desk has a sharp edge I have to avoid. Most important -- I've learned to listen to my hands. If I'm starting to feel pains, it's probably a good day to catch up on journal articles, rather than to start writing a paper.

--Steve Bellovin

[I don't think I ever mentioned to you all that I got one of our tech wizards to rig up foot pedals for the CONTROL and META keys, so that I could practice my organ-pedal action and keep my left wrist/pinky from

spasming in EMACS. It made a big difference.

The following is starkly excerpted by Steve, and is reproduced here despite its length, because of its importance to RISKS. PGN]

EPIDEMIC AT THE COMPUTER: HAND AND ARM INJURIES, by JANE E. BRODY c.1992 N.Y. Times News Service

Work-related injuries, long the plague of those who do heavy manual labor, have become a scourge among white-collar workers, too.

Experts say hundreds of thousands of office workers are being disabled each year in an epidemic of motion-related damage to the hands and arms that is costing the nation many billions of dollars annually.

The problem is expected to worsen in the current recession as businesses demand greater output from fewer employees and workers ignore symptoms for fear of losing their jobs.

Over the last decade disorders caused by movements repeated many thousands of times a day, long a plague on assembly lines and in processing plants, have invaded the once low-risk environment of the office worker along with the computer.

Computer operators spend many hours in the same position doing the same task without breaks or variation, giving no time for stressed tissues to recover.

Over time, this behavior can induce crippling changes in the sensitive tissues of the wrist and hand.

High rates of injury have been reported among data entry workers, telephone operators and newspaper reporters and editors who work for many hours a day typing on a computer keyboard. ...

People with the disorders, which can sometimes be permanent, can find themselves unemployable or forced to change careers. Favorite sports activities, housework, carrying groceries, or even holding a coffee cup may become difficult or impossibly painful.

The disorders have many names -- repetitive stress or repetitive motion injuries, cumulative trauma disorders, of which carpal tunnel syndrome is one, and most recently, work-related musculoskeletal disorders, the designation of the World Health Organization.

But it all boils down to damage caused principally to tissues within the hand and arm by seemingly innocent actions that are repeated perhaps thousands of times each work day, like typing on a computer, cutting meat or poultry or etching glass. ...

The American Academy of Orthopedic Surgeons estimated in 1984 that the problem cost the nation more than \$27 billion a year in lost wages and medical care, an amount that could well have doubled by now since there has been more than a doubling in reported cases.

Dr. Marvin J. Dainoff, a psychologist who is the director of the Center for Ergonomic Research at Miami University in Oxford, Ohio, has called repetitive stress injury the ``occupational disease of the 90s'' similar to the asbestos crisis of the 1980s. ...

"Those with problems that are caught early can expect to recover in a few months," said Dr. Emil Pascarelli, director of ambulatory care at [St. Luke's-Roosevelt Medical Center]. "But workers with severe injuries can take a year or more to get better."

In some parts of the country, workers diagnosed with carpal tunnel syndrome are often treated with surgery to reduce pressure on the nerve that is compressed by swollen or enlarged tissue passing through the wrist.

While some surgeons say the procedure is remarkably helpful to 60 to 80 percent of patients, other experts say it is abused by doctors who do not try

more conservative remedies first. Carpal tunnel surgery is now the second most common operation performed in this country. ...

But repetitive motion disorders received only a flicker of expert attention until they began striking white-collar workers and especially newspaper reporters, who had been all but immune to the job-related injuries that other laborers have endured for centuries.

Some of the rise in cases is widely attributed to increased recognition of the problem and a new willingness to report it.

Dr. Laura Punnett, an ergonomist and epidemiologist at the University of Massachusetts at Lowell, said ``historically there's been lots of underreporting'' of these disorders. As she explained, ``Many workers did not recognize the problem as being job-related; others who did worried about losing their jobs if they reported their injuries.'' ...

A common experience of workers in America who report hand and wrist injuries to their employers is to find themselves suspected of malingering.

Employers' doubts are bolstered by the fact that victims of repetitive stress injury take longer to recover and are less likely to return to work if they have filed worker's compensation claims, according to a study of 28,000 workers conducted by Dr. Gary Franklin, a neurologist who serves as medical director for Washington State's Department of Labor and Industries.

Franklin also noted that the disabilities suffered by many workers were "out of proportion" to measurable abnormalities in their wrists, a widely acknowledged finding that has prompted Nortin M. Hadler, a rheumatologist at the University of North Carolina, to dispute whether the problem is real.

Hadler maintains that musculoskeletal activity that is ``reasonable, comfortable and customary and which can be repeated without undue distress," such as typing on a computer, is unlikely to result in tissue damage.

Others, like Silverstein, report that although dissatisfied workers are prone to exaggerate their injuries or discomforts, she found in studying workers with problems at Newsday that the most devoted and talented reporters typically suffered the most.

"These are high-production people who don't listen to their bodies," Silverstein said. "They don't stop working when they start hurting. The same with musicians. It is the high-performance people who are at highest risk of musculoskeletal disorders. And one could hardly accuse musicians of seeking to get paid without working, since they don't."

In a seven-industry study of factory workers, she also found no differences in overall job satisfaction and in views about work in general among employees afflicted with hand-wrist disorders and those who were not.

Still, she and Franklin agreed that psychological and social factors can make work-related muscular stress worse by increasing muscular tension. ...

Among the physical factors Dainoff lists as raising a worker's risk of hand-wrist disorders are these:

High rates of repetition of the same action. A computer operator who types 60 words a minute can make 18,000 keystrokes in an hour.

Awkward or unnatural posture while working. The ideal position of the wrist is flat and straight, which positions the hand level with the arm and extended in a straight line from it. Those who work with hands bent up, down or to the side risk damage to the tissues in the wrist.

Use of excessive force while working. In Silverstein's factory study, workers who had to use high force and a high rate of repetition had 29 times the rate of hand-wrist disorders as workers using low force and a low rate of repetition.

Lack of adequate rest periods or recovery time. Experts estimate that hands should be relieved of repetitive motion for at least 15 minutes every 2 hours to reduce the risk of injury.

"Try telling that to a reporter writing against a deadline," Silverstein remarked.

People who work on computers, which do not require much force to operate, may nonetheless fall victim to repetitive stress injuries.

Dainoff explained that in many computer-reliant offices like newsrooms, almost every activity is done with the keyboard, including writing, editing, taking notes, searching for information and sending messages. ...

Some computer-based jobs are ``the sweatshops of the 90s," said Dr. John Kella, a musician and biomechanic who directs a rehabilitation and retraining program for injured workers at the Miller Institute in New York.

He pointed out that computer keyboards are unforgiving and many operators press the keys too hard, causing an almost imperceptible kickback as the fingertips hit the keyboard's rock-hard bottom. [In my own personal opinion, keyboard feel has gone vastly downhill since the days of the IBM Selectric typewriter. --smb]

His colleague, Pascarelli, likened it to dancers performing day after day on a concrete floor. ``Eventually, they are going to get injured," he said.

The injuries that he treats are often not ``classical'' syndromes with readily identifiable pathological changes in structures of the hands and wrists.

Some, perhaps a quarter of those complaining of symptoms, have clear cases of carpal tunnel syndrome.

Some have tendinitis, an inflammation of the tendon that passes through the wrist, and others have tenosynovitis, an inflammation of the sheath around the tendon. But many fit no recognized classification.

Dr. Lawrence Fine, an occupational medicine specialist for the National Institute of Occupational Safety and Health in Cincinnati, said: ``Yet these people are in a lot of pain and are forced to take time off from work. It's hard for me as a physician to say it's all in people's heads, especially when the frequency and severity of the disorders abates when the risk factors are reduced.''

Even when a rational remedy is applied, the workplace setting can sometimes cause it to backfire.

Silverstein gave on-the-job exercises to workers in a dental floss manufacturing plant.

A year into the program she found no improvement in the rate of repetitive stress injuries because the workers, forced to meet production quotas, had worked harder to make up for the time lost during their exercise sessions.

COMPUTER USERS' INJURIES ARE OFTEN PREVENTABLE By JANE E. BRODY c.1992 N.Y. Times News Service

Researchers who have analyzed the conditions that seem to lead up to hand-wrist problems and clinicians who treat them have identified factors both within and outside the workplace that when properly adjusted can help prevent hand-wrist injuries.

Dr. Marvin J. Dainoff, director of the Center for Ergonomic Research and a professor of psychology at Miami University in Oxford, Ohio, insists that physiologically sensible use of the computer starts with the user's chair.

A well-designed chair not only helps protect your back but also reduces

====

strain on your shoulders, neck and arms and ultimately your hands.

Most experts recommend a chair that allows you to adjust the height of the seat and the tilt of the back and possibly also of the seat. An adjustable table may also be necessary for people who are very tall or very short.

You should be able to sit with your feet flat on the floor (or on a footrest), your thighs at right angles to your torso, your arms and hands parallel to the floor or perhaps slightly elevated, your head erect and your eyes looking slightly down (about 15 degrees below the horizontal) to see the screen.

To minimize stress, the chair should support your lower back and should swivel and roll on casters. To allow for relaxation of muscles and shifts in working postures, the seat back should be able to tilt backward to an angle of 15 degrees or more from the vertical.

The desirability of arm rests is a matter of debate. Some experts suggest they can aggravate wrist problems and encourage poor posture if the arms are rested on them while typing. Others laud their usefulness as a resting place when not typing.

Next comes the surface on which the computer keyboard rests. When sitting properly in your chair, you should be able to type with a flat wrist. Avoid bending your wrist up or down or twisting it sideways when you type.

If the keyboard is very wide or deep, learn to lift your hand to reach outlying keys instead of trying to stretch your fingers to them, which distorts your wrist position.

While typing, avoid resting your wrists on the edge of the work surface; to reduce pressure on the wrists, consider using a padded wrist and palm rest in front of the keyboard. Keep fingernails trimmed; long nails force you to extend your fingers to hit the keys.

Try to avoid other potentially wrist-damaging activities when you are not typing. Dainoff cautions against moves that bend the wrist, especially if force is involved, like pushing a heavy door, opening jars, holding a telephone handset at an angle or resting your head in your hand.

Also think about home and recreational activities that might aggravate a sore wrist, including excessive use of a kitchen knife, playing a musical instrument with a distorted wrist, skating with the hand bent up at the wrist or pushing a power mower.

Use your whole hand (not just thumb and forefinger) and minimal force when gripping, grasping or lifting an object.

Take frequent brief rests while typing. Switch to another activity that uses the hands differently. Do not use more force than necessary to hit the keys. When taking notes or writing an original work, avoid holding your hands in a tensed ``ready'' position when waiting to type.

Do exercises that strengthen hand and arm muscles and improve circulation in the upper extremities, like squeezing a handgripper and swimming. When typing, try to rely more on the larger, stronger muscles of the arms and shoulders to reduce strain on the wrists and hands.

When detected and intercepted in their early stages, hand and wrist problems are relatively easy to reverse. Experts caution against trying to work through pain, since that will only make the injury worse and could result in irreversible damage to the nerve that passes through the wrist into the hand.

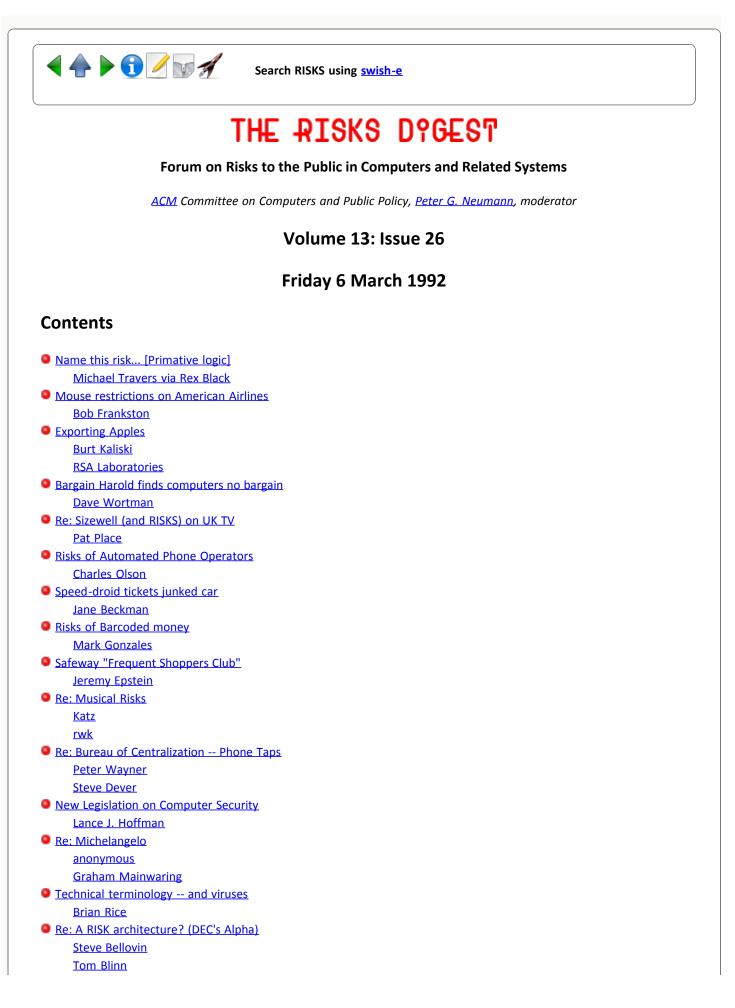
Therapy may involve analysis of your typing technique and retraining, adjustments in your office furniture and keyboard, physical conditioning and the use of wrist splints at night to prevent abnormal wrist positions during sleep. Dr. Emil Pascarelli, director of ambulatory care at St. Luke's-Roosevelt Medical Center in New York, who established a hand clinic to treat injured keyboard users, said that anti-inflammatory drugs, like ibuprofen, do not seem to work well in treating work-related injuries to the wrists and hands.

He also maintains that surgery, which has become a very popular remedy nationwide, should be considered a treatment of last resort, when more conservative measures seem unable to relieve the problem or when the nerve is becoming scarred or is degenerating.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



- Imprecision not considered harmful Eric Sosman
- Info on RISKS (comp.risks)

## Mame this risk... [Primative logic]

Rex Black <rex@devnet.la.locus.com> Thu, 5 Mar 92 10:37:55 -0800

>From: Michael Travers <mt@media.mit.edu>

Toronto, Canada:

Archbisop George Cram enjoys a banana once in a while, but he's not the kind of primate that ape researchers had in mind. The University of Wisconsin's Regional Primate Research Center sent Cram, primate (senior archbishop) of the Anglican Church of Canada, a questionnaire while preparing an international directory of primatology. The envelope was addressed to "George Cram, Primates World Relief and Development Fund."

The Reverend Michael Ingham, secretary for the senior archbishop, suggested in a letter of reply that "primates in your study are perhaps of a different species. While it is true that our primate occasionally enjoys bananas, I have never seen him walk with his knuckles on the ground or scratch himself publicly under the armpits," Ingham said. "There are a mere 28 Anglican primates in the whole world," he said. "They are all males, of course, but so far we have had no problems of reproduction."

The research center's director, John Hearn, promised to strike the church from a computer database and added in a letter to Ingham; "In our zeal to develop a comprehensive directory, we have strayed on this occasion from the arboreal to the spiritual."

#### Mouse restrictions on American Airlines

<Bob\_Frankston@frankston.std.com> Fri 6 Mar 1992 12:52 -0500

Date: 03-03-92 07:59:18 PM MEMO From: John Bartlett [WITH PERMISSION TO RISKS]

I'm sitting on an American flight to Dallas working on a presentation for tomorrow and I can't believe what I've just been told. A flight attendant came over and politely said that it was ok to use my portable (Compaq LTE) on the plane but that according to a new regulation, I would not be able to use my mouse (Microsoft ballpoint)! I of course thought she was joking but apparently according to a new regulation only portables with a built-in mouse are allowed. She actually showed me the regulation which specifically states that mice with umbilical cords can't be used because of interference with flight navigation systems.. This basically limits the use of mice to Mac Powerbooks and a few obscure portables. Using Freelance without a mouse is just about impossible. I tried to argue that there wasn't any difference between a mouse connected with a cord and one that is internal. The flight attendant spoke to the captain in this instance let it go but all should be aware of this new American policy when flying.

#### Exporting Apples

Burt Kaliski, RSA Laboratories <burt@RSA.COM> Fri, 6 Mar 92 15:33:22 PST

The Wall Street Journal, "Apple Computer Backs Technology of Two Companies," by G. Pascal Zachary, March 4, 1992, states:

In connection with its support for data encryption, Apple said it had applied to the U.S. Commerce Department for the right to export software containing the technology, which is generally restricted as a sensitive technology. Apple said it expects to receive export approval because the National Security Agency, a leading agency on cryptographic policy, has reviewed the design and raised no objections to it.

> [The two companies are Adobe and RSA. The Tail of Two Companies may wag the dog. Apple's InCider? PGN]

#### Margain Harold finds computers no bargain

Dave Wortman <dw@swatter.fly.toronto.edu> Fri, 6 Mar 92 13:08:35 EST

Bargain Harold's, a local discount retail chain has just been petitioned into receivership by its creditors. 160 stores across Canada will likely be closed. There are several RISKS related reasons for this situation:

- new management spent \$15M on store refurbishment and on a computerized point-of-sale system with centralized inventory management. This was \$7M more than was authorized by the companies creditors.
- the companies immediate financial difficulties are being blamed on several factors including undetected errors in the new management information system. Apparently this system was incorrectly predicting gross margin on sales and profits. Based on this incorrect information management built up excessive inventories and were unable to reliablely predict the company's annual profit. A profit estimate of \$500K on Oct 2 was changed the next day to a estimated loss of \$3-4M. The projected loss grew rapidly over the next few months (currently \$20M).

Details on the reasons for the MIS system failure are not yet available.

## Re: Sizewell (and RISKS) on UK TV

Pat Place <prp@sei.cmu.edu>

#### Fri Mar 06 08:56:40 1992

I have not seen the Channel 4 TV program and cannot comment on the angle taken in that presentation. However, the impression I am getting from this forum is that the only protection mechanism for Sizewell B is the 100,000 lines of code software system, about which we could reasonably be concerned.

I would like to point out that I have been led to believe that a secondary protection system exists that also has the capability of shutting down the reactor and that this secondary system is a more traditional hardware based system. Further, I have been told that these two systems are independent. So, before we raise concerns over the safety of Sizewell B, can we have all the facts relating to the protection mechanism and not just the worry over the software?

Pat Place prp@sei.cmu.edu

#### Kisks of Automated Phone Operators (RE: <u>RISKS-13.24</u>)

<olson@husc.harvard.edu> Thu, 5 Mar 92 23:16:04 -0500

Our moderator's comments about the potential fraud problems with AT&T's operatorless collect-call system reminded me of my one experience with it. I had to call AAA, for the obvious reason that the car I was traveling in had decided to fry its clutch, and they tell you to call collect. The conversation ran as follows:

Me: [Dial 0 + number]
Pleasant recorded voice: "...If you are making a collect call, please press `1-1' now." [or some such]
Me: [Key 1-1]
Voice: "Please say your name."
Me: "Charles Olson"
Voice: "Please wait while we determine if your call will be accepted..."
[brrrring...brrrring....]
[click]
AAA recording: "Thank you for calling | AT&T recording: "You have a collect
AAA Emergency Road Service. We will | call from [my voice] Charles Olson.
accept your collect call. If you... | If you accept this call, please...

Me: "AAARRRGGGHHHH!!!!!!" [SLAM!]

#### Speed-droid tickets junked car

Jane Beckman <jane@stratus.swdc.stratus.com> Thu, 5 Mar 92 18:59:58 PST

I snagged this one from the alt.folklore.urban group, but it doesn't seem to be a legend, but rather a risks illustration. There are already lots of cars out on the road, where the new owner has never bothered to file the change of ownership (why you should always go with a buyer to re-register the car). But a junkyard? How many states don't have any provision for the owner declaring the car dead, but rely on a possibly unscrupulous junkyard to send in paperwork (and/or plates)? Having sold a junked car myself, once, I wondered about whether the change of title would actually be sent in, or if there was a black market for plates. (My understanding of California law is that sending in the "I've sold it" slip to the DMV does not actually modify the computer records on the car. That must be done by title change. I have no idea what the procedure may be in other states.)

Also, it brings up the issue of identity, when a car is "salvaged," and the only witness who can establish an identity for the driver is a camera. In a manned pullover, the cop asks for a driver's license and checks it against the registration, and if the owner isn't in the car, that person had better have a good story. There is no hope of catching a person who is operating a vehicle illegally if the only enforcement is robotic.

Jane Beckman [jane@swdc.stratus.com]

Ghost Car Speeding? Photocop Snaps Auto 'Retired' 8 Months Ago By Stephen Hunt, The Salt Lake Tribune [last month sometime]

Susan Johnson laid to rest her 1984 Toyota Tercel eight months ago. The car had 200,000 miles on it. When it quit running in June, she sold it to a wrecking yard for \$50. She was sure she'd seen the last of it.

But according to a traffic ticket Ms. Johnson received in the mail last week, the car has been resurrected and is speeding about the streets of West Valley City. The ticket says Photcopy -- a computerized ticketing system that snaps pictures of speeding carss -- caught the car traveling 47 miles per hour in a 35 mph zone on Jan. 10.

Since the car was not even running last time she saw it, Ms. Johnson is wondering how it could be breaking speed laws. "I was so surprised," she said. She believes someone must be using her old license plates, which were left on the car when she sold it.

According to Utah law, license plates are to be returned to the state Motor Vehicle Division when a car is sold. However, once the title has been signed and delivered to the new owner, the previous owner is no longer liable, according to the DMV.

Ms. Johnson was to appear today in West Valley City 5th Circuit Court to deal with the ticket. There, she will be allowed to see the photo and, she hopes, prove her innocence.

Photocop uses radar, a computer and a camera to snap pictures of speeders that show both the car's license plate and the driver. "I hope it's not someone who looks like me," Ms. Johnson said.

Photo radar has become a controversy at the Legislature. Two bills regarding the device are before lawmakers. One would limit the use of photo-radar to school zones only; another would ban it altogether.

Opponents say Photocop smacks of Big Brother.

Imagine That!

Bert Nelson, Weber State University, bnelson@csulx.weber.edu

## Risks of Barcoded money

<markg@ichips.intel.com> Wed, 4 Mar 92 12:06:52 PST

The Nova show on PBS last night (3 Mar 1992) was about banknote printing technology, covering the endless battle between the banknote printers and the forgers.

One interesting item they mentioned in passing was that some new Dutch banknotes have a barcoded serial number, supposedly as a means of detecting forged notes, which would have a duplicated, or unused serial number. Whenever a batch of notes gets back to the central bank all their serial numbers are checked by computer.

The RISKS of this are pretty obvious. Cash will no longer allow anonymous transactions. It would be a simple step for ATMs to make a record of the serial numbers of all notes they issue to each customer. It would also be simple and 'logical' for stores and supermarkets to use their bar code scanners to check the serial numbers of notes they receive (in case of forgery).

The Police could also check the numbers of notes they confiscate in connection with crimes. Then citizens would have to explain why a bank note they were issued by an ATM at 08:31 on 1/2/99 was found on the person of a drug dealer at 11:20 on 1/2/99, while no stores have records of that note being spent in the intervening hours: "If you did not spend the money at an authorized retail outlet, what did you do with it, sir?"

Barcoded bank notes was a pretty obvious step, but it seems to me that the unpleasant civil liberties consequences to us all far outweigh the benefits of catching a few forgers.

Mark Gonzales

## ✓ Safeway "Frequent Shoppers Club"

Jeremy Epstein <epstein%trwacs@uunet.UU.NET> Thu, 5 Mar 92 10:41:23 EST

Safeway stores in the Washington area (and perhaps other areas) recently introduced a "Frequent Shoppers Club". By filling out a form which includes various demographic and financial information, you get discounts (typically 10%) on a few sale items each week (i.e., 10% below the price offered non-members). There's no cost to join the club.

Safeway is obviously trying to build a database of buying habits which can then be resold to advertisers for targeted advertising. Many people are up in arms about "invasion of privacy". Safeway has a program now where every time you use your frequent shoppers card, you're automatically entered in a mini-lottery (to encourage use of the card).

What strikes me as curious is that people don't seem to realize that the RISK is already there. With UPC scanners coupled with check cashing cards, there's already the opportunity to gather and correlate the information for a large fraction of the population. Are there any laws which prevent the grocery store from selling that information? The check cashing application forms don't preclude the store from doing whatever it wants with the non-financial information. Are there any instances of stores which actually do the correlation and resell the information?

I'm also curious what reactions have been to these sorts of programs in other parts of the country/world.

Jeremy Epstein, Trusted X Research Group, TRW Systems Division, Fairfax, Virginia +1 703/803-4974 UUCP: uunet!trwacs!epstein

#### 🗡 Re: Musical Risks

<katz@merit.edu> Thu, 5 Mar 92 18:52:26 EST

The obvious solution to the DX-7 dilemma is to sample the patches used in the performance using a sampling synthesizer. Of course, something is lost in the process (especially if the timbre is modified dynamically). You could always sample the entire performance, of course, but then you may as well just roll a tape.

The band Pere Ubu seems to have left its old Moog synth (knobs and patch cords and all) behind on the last tour, but not before sampling it into a slightly more modern synth.

## Ke: Musical Risks (<u>RISKS-13.25</u> [so-called])

<rwk@crl.dec.com> Thu, 5 Mar 92 21:24:46 -0500

Geoff Kuenning discusses the risk of not having DX-7s available to classical music in 20 years time.

(Hmm, mine's about a third of the way there and still going strong).

Anyway, it's really not that hard to do a DX-7 in software if you have the processing power. In twenty years, I'll expect my wristwatch to have that much processing power, if not my athletic shoe!

# Ke: Bureau of Centralization -- Phone Taps

Peter Wayner <wayner@cs.cornell.edu> Fri, 6 Mar 1992 18:16:20 GMT

USA Today reports in Friday, March 6th paper that the Dept. of Justice is floating a proposal that would require phone companies to centralize phone tapping and make it easier for law enforcement agencies to listen in. They note that this would raise monthly phone bills for all consumers.

Peter Wayner Department of Computer Science Cornell Univ. Ithaca, NY 14850 EMail:wayner@cs.cornell.edu Office: 607-255-9202 or 255-1008

# Ke: Bureau of Centralization -- phone taps

Steve Dever <Steve.Dever@eng.sun.com> Fri, 6 Mar 92 13:34:48 PST

The 6-Mar-1992 San Jose Mercury News has an article about this on page 5A. The article is titled: "White House wants consumers to pay bill for better wiretaps." According to the article, the Justice Dept. is worried that "the widespread use of digital transmission, fiber optics and other technologies" make it difficult for government agencies to intercept transmissions. The Justice Dept. is proposing a bill which would direct the FCC to "devise rules to give law enforcement agencies access to conversations for court ordered wiretapping." Phone companies would then be required to follow the rules. The bill would also authorize the FCC to permit the phone companies to increase rates to cover the cost of implementing the rules.

The proposal has been discussed with Sen. Ernest Hollings, chair of the Senate Commerce Committee which oversees the FCC.

Steve Dever

# Ke: Bureau of Centralization -- phone taps

Peter Wayner <wayner@cs.cornell.edu> Fri, 06 Mar 92 17:03:12 -0500

I've had a few second-order thoughts about the matter.

0) The Justice department seems to want to ensure that there is some place in the system where the signal can be easily turned into sound. It does not seem to prohibit individual people from encrypting their messages. It just means that the phone company needs to provide a tap.

1) Centralized phone tapping doesn't necessarily mean less privacy. I can imagine a huge bureaucracy at the local phone companies' tap center filled with mean clerks who would demand to see the proper forms authorizing the taps. "No, I'm sorry Officer. You didn't submit 44/22-G that authorizes the recording of conversations from another state that are forwarded to a third state by a

central routing office without being delivered to the phone in your juristiction. A 44/22-F authorizes only cross-county juristiction expansion."

Now each police department probably has its own set of mikes and tape recorders and can place them as it wishes.

2) I don't necessarily believe that the above will happen.

#### New Legislation on Computer Security

Lance J. Hoffman <hoffman@seas.gwu.edu> Fri, 6 Mar 92 12:16:38 EST

Recently introduced legislation may be of interest to RISKS readers. S. 2198, the Intelligence Reorganization Act of 1992 and HR 4165, the National Security Act of 1992, essentially give responsibility for all comsec to the National Security Agency and for all information security to them also. This, of course, would completely reverse, existing structure which has just been in place for a couple of years, and apparently take much responsibility away from the National Institute of Standards and Technology (NIST) in the Dept. of Commerce and put it (back) at NSA in the Defense Dept.

If enacted, this would have important implications for export control and crypto policy, which are of interest to many RISKS readers. Lance Hoffman

Department of Electrical Engineering and Computer Science, The George Washington University, Washington, D. C. 20052 (202) 994-4955

## 🗡 Re: Michelangelo

<[anonymous]> Thu 5 Mar 1992 19:34 -0500

I spent the day today clearing many viruses. In the last week xxxx and I have cleared over 80 Michelangelos from .... Also, we have cleared many Cascades, New Zealands, Joshis, and others. Easily over 120 infections in the last week.

You may have heard that just changing the date is an adequate defense; it is not. You may have heard that not using the computer that day is a defense; it is not. You may have learned many things; almost all of them untrue. All anyone needs to know is that Michelangelo is a very widespread virus. It is destructive. It can be removed only by using proper procedures. It is completely manageable and removable.

Procedures:

Detect the virus (Use any commercial or other package that is up to date) Cold Clean Boot (Turn off PC, insert DOS Startup notchless diskette, turn on PC) Copy first track into memory Copy partition table from virus (sector 1) into partition table of original (sector 7) in memory Copy original over virus in memory Zero the copy of the original in memory Write the result back to the first track.

As you can see, nothing magic, just plain old careful procedure.

Anyone who leaves a diskette in their boot drive by accident when they boot should have their wrist slapped.

## Ke: Michelangelo (<u>RISKS-13.21</u>)

Graham Mainwaring <octogard!graham@duke.cs.duke.edu> Thu, 05 Mar 92 22:10:45 EST

In <u>RISKS-13.21</u>, jcav@midway.uchicago.edu writes about his local news station omitting to mention that the Michelangelo virus only affects MS-DOS machines. I submit that this really isn't much of a problem, for the following reasons:

1. MS-DOS users are actually affected by the virus, so in their case, the report was correct and useful.

2. Macintosh users have such a frightening virus problem already that there are very few left who don't routinely disinfect their machines.

3. Everyone else is either sophisticated enough to understand the situation, or has a MIS department to call and get straightened out by.

A more serious problem is the entire area of media handling of Michelangelo. Why is this particular virus getting almost saturation-level coverage in the media? Is Michelangelo really any worse than Stoned, 1701, Jerusalem-B, or any of the other MS-DOS viruses that have been circulating lately?

Even worse, will people assume that once they have scanned their disks for Michelangelo, that the threat is over? After all, the fuss has quieted down. Why should it be necessary to do it again?

Internet: octogard!graham@deepthot.cary.nc.us BBS: +1 919 876 7213 UUCP: ...!duke!wolves!deepthot!octogard!graham WWIVnet: 1@9970

## ✓ Technical terminology -- and viruses

Brian Rice <rice@dg-rtp.dg.com> Fri, 6 Mar 1992 14:16:41 -0500

Here's another one for the "risks of posting to RISKS" file.

In <u>RISKS-12.30</u>, 11 Sep 1991, I wrote, concerning so-called beneficial viruses:

"...the idea of code roaming around in a network looking for opportunities to do good is what we technical types call `way cool.'"

In \_Newsweek\_, 20 Jan 1992, John Schwartz writes, concerning virtualreality video games:

"When you shoot, your nemesis is blown to colorful smithereens-a sight that is, to use a technical term, way cool."

It's just like William S. Burroughs said: "Language is a virus."

Brian Rice, DG/UX Software Quality Assurance, Data General Corp., Research Triangle Park, N.C. rice@dg-rtp.dg.com +1 919 248-6328

## Ke: A RISK architecture? (DEC's Alpha)

Steve Bellovin <smb@ulysses.att.com> Thu, 05 Mar 92 19:30:01 EST

Brian Randell describes how the Alpha uses imprecise arithmetic traps, and speculates that it's a risk to program correctness. With all due respect, I disagree. Based on my experience with imprecise interrupts on the 360/91, lo these many years ago, I would classify imprecise interrupts as more of a hassle when localizing faults, rather than any risk to the program's correct behavior. That is, the interrupts -- which typically signified erroneous program behavior -- still happened, and still caused the program to abort. But it took rather more debugging effort to figure out which instruction caused the trap. Unless one is relying the interrupt handler to perform the appropriate fix-up -- a technique that I regard as far more risky and non-portable than imprecise interrupts -- correct programs should not behave any differently.

He also describes the barrier instruction as a ``sop to DEC's technical conscience". Not so. Its purpose is to help the programmer identify the offending instruction. And compilers can (and were able to) generate such instructions on appropriate boundaries. I recall vividly, 20+ years later, finding that a zero- divide fault took place 11 instructions after the offending divide, and after the divisor register had been overwritten with a non-zero value. But it had to be that instruction; there were only two divide instructions in the entire program, and the other referenced a still-intact constant.

If there is a danger here, it's from the hardware design itself. Pipelined architectures imply parallelism, of course, and that's harder to get right. But the hardware designers seem to do a better job which such things than do the software designers...

--Steve Bellovin

Alpha's "imprecise arithmetic traps" are nothing new..

"Dr. Tom @MKO, CMG S/W Mktg, DTN 264-4865 05-Mar-1992 1834" <blinn@dr.enet.dec.com> Thu, 5 Mar 92 15:46:23 PST

In <u>RISKS-13.25</u> (Thursday 5 March 1992) Brian Randell writes about the new Alpha RISC architecture and comments on its imprecise arithmetic traps.

Those of us who ever programmed the IBM System/360 Model 91 under OS/MVT (or, I'd imagine, other OSes) will recall that it, too, had imprecise interrupts, in large part because it provided (limited) pipelining and multiple issue of arithmetic instructions. I don't recall the details -- it has been a long time -- but as I recall it could overlap integer and floating point compute operations, and perhaps did multiple floating multiplies in parallel. In any case, the careless programmer could easily get the dreaded OC5 ABEND, along with a generally useless dump, when one of the parallel operations failed.

IBM, in their infinite wisdom, did not provide a Trapb instruction to allow the programmer to force precise interrupts -- at least, I don't recall any such instruction. Instead, if you couldn't guess what was wrong by looking at the code, you could carry it to a different System/360 model (like the Model 75) that didn't provide the parallelism and get a precise interrupt.

What's neat about the Alpha design is, of course, that you can get precise traps when you need or want them, at some performance penalty, but you can go blazingly fast when you don't need that precision. Compared to other ways of addressing the problems implied by a pipelined multi-issue architecture, the Alpha approach seems rather clean and clever to me. But then, I may be biased, and I'm not an experienced computer architect.

Dr. Thomas P. Blinn, Digital Equipment Corporation, Digital Drive -- MKO2-2/F10 Merrimack, New Hampshire 03054 ...!decwrl!dr.enet.dec.com!blinn (603) 884-4865

#### Imprecision not considered harmful

Eric Sosman x4425 <eric@tardis.hq.ileaf.com> Fri, 6 Mar 92 09:49:45 EST

In <u>RISKS-13.25</u> (so-called), Brian.Randell@newcastle.ac.uk seems alarmed at the notion of imprecise delivery of instruction exceptions. I was similarly alarmed when I first heard of them ... twenty-plus years ago, with the IBM System/360 model 91. (I'm not claiming the 91 was the first such implementation, simply that is was the first in my personal experience.)

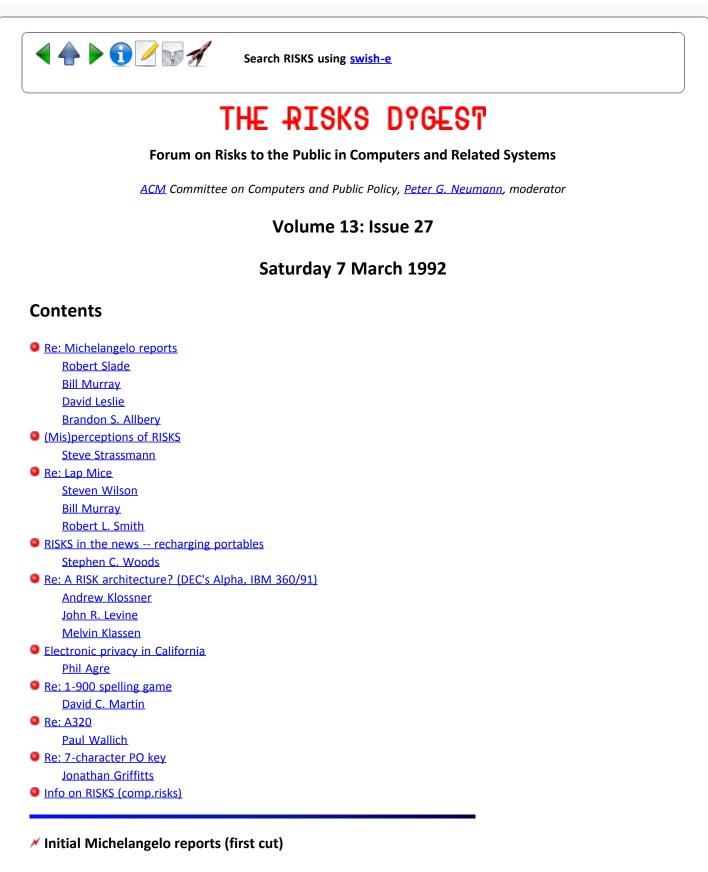
It is only sometimes useful to identify "the" instruction which blew up; usually a coarser localization will do. The imprecise-exception architectures I know of all provide an instruction which acts as a barrier, with the promise that no exception delivered after the barrier can be due to any instruction fetched before the barrier. The 360-91 used "BR 0,0": a "no-op" in the form of a pipeline-draining conditional branch. Compilers inserted this instruction at strategic locations like subroutine prologues and epilogues, or (if requested) between segments of code generated for different source statements. Imprecise exceptions make it difficult to write trap handlers which fix up the results of failing instructions. I have written such handlers, but have never found them satisfactory -- the "correct" fix is too context-dependent to be dealt with by such a low-level approach. Error detection and correction work much better in the higher levels, and imprecise instructions don't make the superior approach impossible or even difficult.

Eric Sosman eric@hq.ileaf.com Interleaf, Inc. / Prospect Place, 9 Hillside Ave. / Waltham, MA 02154



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Robert Slade <rslade@sfu.ca> Sat, 7 Mar 1992 22:49:30 GMT

To all who sent in reports, many thanks. A brief report on today (and recent past) sightings:

New Zealand - our two best contacts evidently did their job well, and had clean shops. Other areas reported a "detection rate" (in advance of the deadline) of 10% in some areas.

Japan - MITI had stated earlier in the week that Japan would not be hit as it didn't use MS-DOS much. MITI, and seven other companies, reported hits today. (MITI only reported one.)

China - announced hits in spite of official claims of "about 10" reported occurrences.

Poland - earlier in the week was reporting detection rates of as high as 25%

Germany - reported heavily hit by CBC, conspicuous by the absence of reports from Vesselin. Too busy? :-)

South Africa - reported by CBC to have had 1300 hits.

US - New Jersey Institute of Technology reported to have cleaned 2400 of 3000 computers earlier this week (est. cost = \$60,000, mine) - largest oil company in Houston, and 200 small to mid sized businesses (est. cost for recovery of computers, assuming backup, \$2M, mine)

- eastern university reporting a couple of hits

Canada - major metal supplier "tested" for the virus by playing "Michelangelo roulette" (setting date ahead to Mar. 6) late last night, lost that machine and cleaned up the rest. Two Baptist churches reported hit in the Vancouver area. Local school board found a copy on one machine, tested on old machine, did not trigger, figured Mikey was a hoax. (Any bets the test machine was a really old XT? Wonder if they got hit and are now lying low.) UofA reports one hit (good work, Tim), NRC reports four disks cleaned.

In other news:

McAfee is quoted as saying clocks on machines that triggered on Thursday (a fair number of reports of that) were set ahead by "accident". No one is reporting the significance of the leap year.

A number of reports of users playing Michelangelo roulette, including one that lost a full 170M hard disk (170 "shelf feet" of printout, gone). Another found the virus, tried to disassemble it with DEBUG, and triggered it.

A number of reports of CLEAN and the NAV Special Edition "damaging" disks and partitions. No report of the fact that NAV Special does not check for any other virus. (CPAVSE checks for some "Friday the 13th" families, at least.)

Very few reports of the upcoming Thursday the 12th, Friday the 13th, Saturday the 14th, Maltese Amoeba next week.

Story of the year:

One user supplied a copy of a detection program to his sister, who found the

virus at the radio station where she worked (in Quebec). He called the corresponding station nearby, and offered to scan their computers. They turned him down, stating they were sure they did not have the virus.

This morning, they powered up and lost the hard drive.

Sorry for typos and terse style, trying to keep up and get reports out at the same time.

Vancouver Institute for Research into User Security Canada V7K 2G6 rslade@cue.bc.ca Robert\_Slade@sfu.ca CyberStore Dpac 85301030

PS - latest reports, John M. estimating 10,000 hits world wide, one newswire carrying estimate of 400,000 in US. Shall we start the Mikey

#### Measuring Michelangelo

<WHMurray@DOCKMASTER.NCSC.MIL> Sat, 7 Mar 92 09:44 EST

... I suspect that we will detect and eliminate far more copies of other viruses than of Michelangelo.

The sense of urgency generated by Michelangelo's trigger date (I received calls right up to midnight on the 5th) has resulted in the purchase, use, and, I hope, permanent installation of a great deal of anti-virus software. How many more copies might we have eliminated if our advice had focused on infected diskettes as much as it did on infected machines.

Unfortunately, we have not stamped out viruses. We will have such an opportunity again. I suggest that the next time we have the public's attention, we focus on diskettes. It is diskettes that hold the majority of the copies of viruses and it is on dikettes that they are most persistent.

Later in his posting, Joe Abernathy asks for reports of Michelangelo. I expect those to be sparse. (Joe, add Hoyt Limousine of New Canaan to your list (I got that report as a customer, not as a consultant)). I think that the estimates of the number of copies that Michelangelo achieved in a year were generally exaggerated, and the purge more effective than I would have hoped. I do not begrudge the bold and brave entrepreneurs that gave us the software their sales. I think that the press coverage was at least partially motivated by a spirit of public service. But by any count, the security costs of Michelangelo will be much higher than the cleanup, and mammoth by any measure.

William Hugh Murray, Executive Consultant, Information System Security 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

#### MichelAngelo virus less a risk than Norton

## David Leslie <dleslie@phakt.usc.edu> Sat, 7 Mar 92 15:24:00 PST

As the hype surrounding the MichelAngelo virus reached a peak, Norton released a 'special' version of its virus utility (free of charge) to the public. This special version was limited to check and remove the MichelAngelo virus. Unfortunatly for myself and many others who received this software, it turns out to be more dangerous than the virus. If you use the norton utility to remove the virus from a harddrive with more than 1 partition, you may very well lose all but the first partition. I believe this may have something to do with using alternate filing systems. We lost 3 40 meg partions(d:,e:,f:). I have heard as many reports of people losing partitions due to Norton as to MichelAngelo. Beware of the undocumented 'features' of the Norton virus utility :(

David Leslie dleslie@girtab.usc.edu

#### Ke: Michelangelo (Mainwaring, <u>RISKS-13.26</u>)

Brandon S. Allbery KF8NH <allbery@ncoast.org> Sat, 7 Mar 92 14:24:33 -0500

| Even worse, will people assume that once they have scanned their disks| for Michelangelo, that the threat is over? After all, the fuss has| quieted down. Why should it be necessary to do it again?

Worse, the media blitz left out information that caused companies to lose time due to unnecessary fear of the virus. One of our customers refused to bring up his computer on Friday out of fear of the virus; he knew enough to know it was an Intel 386-based computer, therefore it "must" be vulnerable.

The computer in question was an Altos Computer Systems, Inc. 386/2000. It is completely incompatible with MS-DOS and does not possess a BIOS --- it has a bootstrap loader/monitor and self-test facility in ROM, and nothing else. If someone were to attempt to boot an MS-DOS diskette in it, it would read track 0, not find the information required by the 386/2000, and reject the boot attempt without executing any code off the floppy. And even if someone managed to fake a 386/2000 signature, the first attempted BIOS call would cause an immediate dump into the monitor with an undefined interrupt. And an attempt to access the disk controller directly would find nothing whatsoever, as the disk controller is accessed entirely differently. For all that it's the right processor, the Micheelangelo virus ad as good a chance of infecting a Macintosh as it did this system.

Other customers on 386-based Series 1000 and 2000 machines were also worried, although none took it to quite the lengths that that one customer did (a phone call was sufficient to reassure the others, although some of them waited until noon to call). I didn't hear about any calls from users of Altos 8086 or 80286 machines, which are also incompatible.

So how many other companies needlessly lost the use of their computers? The RISKs of a computer virus are not limited to the systems it infects.

Brandon S. Allbery, KF8NH [44.70.4.88] Senior Programmer, Telotech, Inc.

## // (mis)perceptions of RISKS (Mainwaring, <u>RISKS-13.26</u>)

Steve Strassmann <straz@cambridge.apple.com> Fri, 6 Mar 1992 20:34:12 -0500

2. Macintosh users have such a frightening virus problem already that there are very few left who don't routinely disinfect their machines.

I can't imagine where you got this idea. While perhaps 1000 or more viruses affect DOS, there are exactly 10 known viruses affecting Macs (plus one that affects only Ataris in Mac emulation mode), No known Mac viruses are explicitly malicious like Michelangelo. While new DOS virus strains appear at a rate of several per week, the last new Mac virus appeared after a hiatus of almost two years.

To say that Mac users have a "frightening virus problem" is utterly irresponsible. The popular press, in giving the impression that all computers are susceptible to DOS viruses, is not much better. Perhaps Macintosh users do take better care of their machines, but I imagine it's because it's easier to do so.

Steve Strassmann, PhDstraz@apple.comApple Computer Avanced Technology GroupCambridge, Mass.

## Ke: Lap Mice (Bartlett, <u>RISKS-13.26</u> [sic])

Steven Wilson <stevew@netcom.com> Sat, 7 Mar 92 09:43:52 PST

This is in response to John Bartlett's post concerning mice employed on a Lap Top during a flight. John is mistaken in saying that there is no difference between an internal mouse and one connected via cord.

Depending on whether the cord is shielded properly and how the connection is made to the PC the unit can act just like an external antenna for all the RF noise that the computer is capable of generating. The computers themselves have probably been qualified with specific I/O devices to comply with FCC class B standards concerning RF radiation. Further, American probably has determined that flight instrumentation can safely handle that level. It has also probably been determined that some mice on some systems do indeed result in radiation from the unit above Class B levels that could be harmful thus the flat-out ban. They don't do it by manufacturer type(to hard to enforce).

Does anyone know if this is an FAA ban or an American Airlines Policy?

Steve Wilson

## Mice with Cords on Planes,

<WHMurray@DOCKMASTER.NCSC.MIL> Sat, 7 Mar 92 11:15 EST

Would God that there were no difference. (I will keep my mouse concealed.) Of course, there is: the mouse cord may act as an antenna, effectively broadcasting any RF from the computer.

William Hugh Murray, Executive Consultant, Information System Security 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

#### Ke: Mouse restrictions on American Airlines

Robert L. Smith <rls@tip.wedge.nt.com> Sat, 7 Mar 1992 16:02:59 GMT

John Bartlett is mistaken if he thinks that "there wasn't any difference between a mouse connected with a cord and one that is internal." Mouse cords do something besides pass signals along: they RADIATE electromagnetic energy at the frequency of the microprocessor clock which, being essentially a square wave, can include powerful harmonics well into the UHF bands. This is still a concern even if the mouse cable is shielded because the laptop's ground is not common with the airplane's.

As an apprehensive passenger, I'm pleased that American identified this hazard before it caused damage.

Fortunately my old Toshiba doesn't have a mouse.

#### RISKS in the news -- recharging portables

Stephen C. Woods <scw@ollie.SEAS.UCLA.EDU> Fri, 6 Mar 92 17:56:43 -0800

Today while I was driving home, listening to the news/traffic station in LA (KNX 1070 KC). What should I hear but a reference to the comp.risks `bulletin board'. KNX has a fellow that does a bit about computers. He referenced the recent issue with the report about long lines for the heads on Aircraft with lots of folks using portables as near as I can remember he quoted verbatim from the article. He also mentioned another article from that issue, but the which one has slipped through my parity errors. He did credit the authors, but not our moderator, sorry 'bout that Peter.

Stephen C. Woods; UCLA SEASNET; 2567 BH;LA CA 90024; (310)-825-8614 UUCP: ...{ibmsupt,ncar!cepu}!ollie}!scw Internet:scw@SEAS.UCLA.EDU

## Ke: A RISK architecture? (DEC's Alpha)

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

Fri, 6 Mar 92 16:50:36 PST

Alpha arithmetic traps (overflow, underflow, etc.) are imprecise...

Nothing new here. This is standard practice in high-performance computer designs, going back as far as the IBM 360/91 of the early 1970s. It's not a RISK because any trap is guaranteed to happen before the first use is made of the result of the arithmetic operation. (In this case, that means the first use of the register that was the destination of the instruction in question.)

The only practical difference between imprecise and precise exception is that you can't report the PC of the offending instruction when imprecise.

-=- Andrew Klossner (uunet!tektronix!frip.WV.TEK!andrew)

## Ke: A RISK architecture? (DEC's Alpha) (Randell, <u>RISKS-13.25</u>)

John R. Levine <johnl@iecc.cambridge.ma.us> 7 Mar 92 15:12:14 EST (Sat)

>Alpha arithmetic traps (overflow, underflow, etc.) are imprecise -- they can >be delivered an arbitrary number of instructions [late]

Imprecise interrupts have been around for a long time. I wrestled with them on a 360/91 in about 1970. The /91 could execute instructions out of order if there weren't interferences among them, but didn't keep enough state to unscramble the mess if one of them failed. There were barrier instructions but they slowed the machine down so much that they were almost never used except at statement boundaries in some debugging compilers.

In practice when you got an imprecise interrupt, your job aborted with a code of SOCO, pronounced "Socko!" You could catch the interrupt, but it was so hard to arrange to repair an overflow (even if you used barriers, the interrupt would usually give you the address of the barrier instruction, not the one that failed) that nobody did. Instead, they inserted tests and prescaling to make sure that interrupts would not occur. I opine that if anything, imprecise interrupts encourage more correct software since you know that you can't recover from errors.

John Levine, johnl@iecc.cambridge.ma.us, {spdcc|ima|world}!iecc!johnl

## // Imprecise Interrupts on IBM 360/91 (Blinn, Sosman, <u>RISKS-13.26</u>)

Melvin Klassen <klassen@sol.UVic.CA> Sat, 7 Mar 92 12:43:52 PST

Actually, the 360-91 used 'BCR mask,0' where the 4-bit value in "mask" \*\*had\*\* to be non-zero to drain the pipeline.

If requested, IBM's PL/I compiler inserted 'BCR 15,0' as the first instruction generated for each PL/I statement, thus limiting any imprecise interrupt

to a single PL/I statement.

## Electronic privacy in California

Phil Agre <pagre@weber.UCSD.EDU> Fri, 6 Mar 92 19:18:10 -0800

California Assembly member Gwen Moore has introduced AB 2674 which requires any state or local agency to notify you when it gives out information about you through an electronic medium. The contact person in Assembly member Moore's office is Bill Julian at (916) 445-8800.

Phil Agre, UCSD

#### Ke: 1-900 spelling game (Tannenbaum, <u>RISKS-13.24</u>)

David C. Martin <dcmartin@fascet.msi.com> Fri, 6 Mar 1992 20:20:43 GMT

Andrew Tannenbaum posted a message about the risks of using a computer to generate tones which would help a person to spell twenty (20) words correctly in two (2) minutes. I have a friend who utilized his Sharp Wizard hand-held computer/calendar/etc.. to win at various sports trivia lines. He used this technique to win a substantial prize from one of these trivia lines which then ended up in litigation. One of the points brought up by the lawyers for the 1-900 operator was (erroneously) that he had done exactly what Andrew discussed -- using a computer connected to the phone to generate the tones of the correct response. The lawyers contended that such a technique removed some of the element of skill from the contest and invalidated the prize.

It becomes interesting to me when you attempt to discern where the utility of either a electronic or paper resource ends (supposedly at least a paper reference of sports trivia in the case above is allowed) and the use of automation for "beating the system" begins. If on-line repositories of information are used to augment a persons ability to perform some task, then is the "skill" of the person performing the task any less?

dcm Molecular Simulations, Inc., 796 N. Pastoria Avenue, Sunnyvale, CA 94086 mail: dcmartin@msi.com uucp: uunet!dcmartin 408/522-9236

## Ke: A320 (Spencer, <u>RISKS-13.24</u>)

Paul Wallich <pw@panix.com> Fri, 6 Mar 1992 20:45:32 GMT

>One must remember that COINCIDENCES DO HAPPEN. ...

I believe that this is fuzzy thinking. Airplane crashes in general are the result of multiple failures; only if \_everything\_ goes wrong do you lose a plane. Thus you can argue that any single crash samples a large number of

things going wrong. To wit, when the first DC-10 crashed with a dropped engine, airworthiness inspectors found potentially lethal cracks in the engine mounting of something like 70 other aircraft. In two cases no one could quite figure out why the engine hadn't fallen off already. (And note, btw, that if not for a) the pilot being untrained in this particular kind of disaster and b) the design flaw of misrouted hydraulic lines, dropping an engine wouldn't have been a big deal.)

Air crashes are the tail of a wide distribution in failures, nonetheless when you start getting \_any\_ numbers up in that tail, it should lead you to worry a great deal about where the median may be drifting. This raises an interesting point for designers of both hardware and software: when you get into very-high-reliability systems, how many of the failures are due to problems whose rates have been specified and characterized, and how many are do to completely unanticipated, unanalyzed features of the design?

paul

#### Re: 7-character PO key

Jonathan Griffitts <jgriffit@isis.cs.du.edu> Sat, 7 Mar 92 00:08:05 GMT

My sister also encountered a variation on this problem. While a grad student, she lived in a house with several other students. As is common for students, the residents of this house move very frequently. When she moved away from this place herself, NONE of her mail was correctly forwarded. When whe enquired about this, she found that a former resident of the house had a similar last name (Griffin as compared to Griffitts), and that there was a forwarding notice still in effect for this other unknown person.

The post office's hashing function was completely unable to distinguish between the two forwarding orders. When my sister finally managed to get her own forwarding implemented, she began receiving Ms. Griffin's mail.

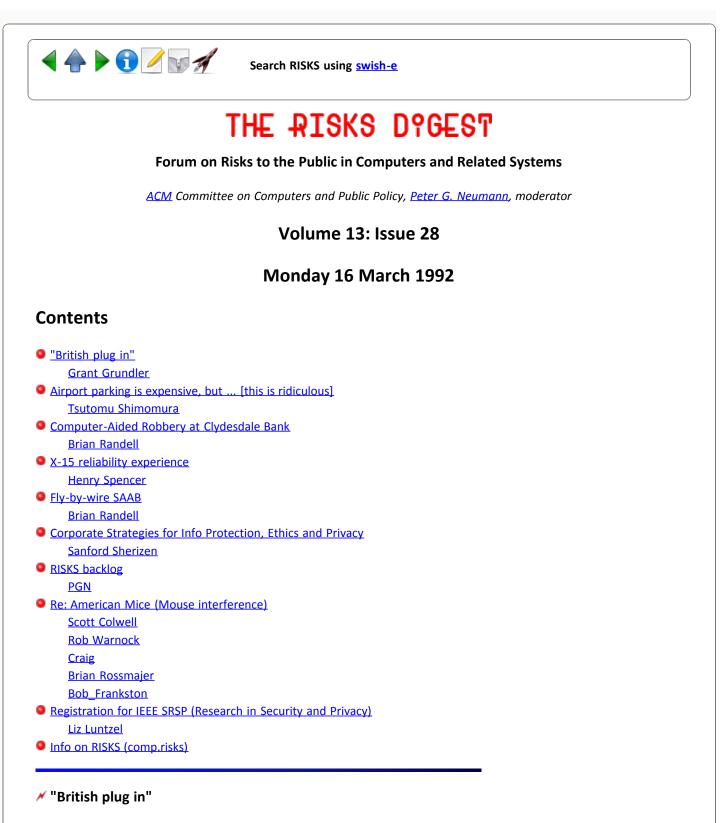
She was repeatedly told by post office employees that this problem was absolutely unfixable within their procedures.

--JCG, AnyWare Engineering, Boulder CO 303 442-0556



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Grant Grundler <grant@oas.olivetti.com> Thu, 12 Mar 92 16:25:55 PST

This is so absurd I should consider submitting it to rec.humor.funny. My guess is a lot of companies put plugs on anyway and the law finally caught up - I just can't imagine it any other way.

The British Plug In (San Jose Mercury News, 2 Feb 1992)

Britain has just announced that makers of electrical appliances in that country must begin to attaching plugs to the ends of electrical cords. Britons, for we don't know how long, have been required to buy plugs and

attach them to their new toasters, irons and electrical what have yous. But now the Royal Society for the Prevention of Accidents, citing its research into the matter, says it was surprised to learn that "it is common practice everywhere else in the world to sell electrical goods with a plug attached."

[And now, a plug for the Royal Society... PGN]

## Airport parking is expensive, but ... [this is ridiculous]

Tsutomu Shimomura <tsutomu@NO-SENSE.LANL.GOV> Thu, 12 Mar 92 15:09:34 -0700

One of the San Diego off-airport parking outfits gave me a "time in" ticket dated February 30 (you can guess the real date). When I returned to retrieve my car on March 6th, I was presented with a demand for \$3771.00 (at \$11/day, \$1/hour), to be paid before I was allowed to leave the lot. The garage attendant decided that this wasn't quite right, reentered the date into his "computer", and was again told that I was to pay \$3771.00. At this point the manager was called for help (the exit line was getting quite long).

I have a receipt here for \$3771.00 for "parking". The travel accounting people are going to have fun with this one... :-)

Tsutomu Shimomura tsutomu@LANL.GOV Los Alamos National Laboratory Los Alamos, NM 87545

### Computer-Aided Robbery at Clydesdale Bank

<Brian.Randell@newcastle.ac.uk> Fri, 13 Mar 92 10:09:10 GMT

The item below is reprinted in its entirety, from today's Independent, a UK national newspaper. I do not recall any previous reports in RISKS of similar cases of in-house "high-tech" cash dispenser robbery - but I must admit I have not followed the stream of cash dispenser stories closely.

Brian Randell

\_\_\_\_\_

#### ROBBER 'FOILED BANK SYSTEM'

An electronics expert stole more than (pounds) 17,000 in a high-tech robbery spree, plundering dozens of accounts from automatic cash dispensers at banks, Paisley [Scotland] Sheriff Court was told yesterday.

Clydesdale Bank chiefs claimed their dispensing system was foolproof and told angry customers that members of their own households must have been responsible for making withdrawals without their knowledge. Anthony Pratt, 32, a bank engineer, used a hand-held computer inside bank premises to record transactions being made by customers at "hole-in-the-wall" machines outside. He recorded the customer's secret number and later used it on plastic cards he made with magnetic strips. Pratt, of East Kilbride, was finally arrested after he took cash from a machine in Glasgow. He admitted conspiracy to rob and robbery. Sentence was deferred for reports until 2 April.

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

## X-15 reliability experience

Henry Spencer <henry@zoo.toronto.edu> Sun, 15 Mar 92 20:11:54 EST

On reading the Proceedings of the X-15 First Flight 30th Anniversary Celebration (NASA CP-3105, Jan 1991), I ran across a section of some relevance to Risks. Insertions in [] are mine.

In 1962, a very comprehensive, but little known, study was initiated by Bob Nagle at AFFTC to quantify the benefits of having a pilot and redundant-emergency systems [this seems to be essentially a buzzword for "redundant systems"] on a research vehicle. Each individual malfunction or abnormal event that occurred after B-52 [X-15 launch aircraft] takeoff for the first 47 free flights of the X-15 was analyzed. The outcome of each event was forecast for three hypothetical models; one with only the pilot but no redundant-emergency systems, one with only the redundant-emergency systems but with no pilot, and one with neither the pilot nor redundant-emergency systems (i.e. single-string [buzzword for no redundancy], unmanned).

[The bar chart of results shows an expected failure rate of over 50% for the "neither" configuration, with many of the failures destroying aircraft. Adding just a pilot or just redundant systems produces only small improvements. Adding both takes the failure rate down to near zero and eliminates aircraft losses.]

[Referring to the graph.] The unmanned, single-string system would have had 11 additional aborts and resulted in the loss of 15 X-15s. [The actual program built only three!] Not surprising is the fact that the pilot is of little value in a system without redundant-emergency systems. He must have some alternate course available in order to be effective. The redundant-emergency systems were also found to be of little value in an unmanned system primarily because the fault detection and switchover logic must presuppose the type of failure or event. For example, few designers would have built in a capability to handle an inadvertent nose gear extension at Mach 4.5.

[That last refers to something that actually happened to an X-15.

Landing gear is normally designed to be extended at a maximum of a few hundred MPH. Having gear extend at 3000+ MPH is a horrifying prospect, but the X-15 was landed safely with minor damage to the aircraft and the pilot unhurt.]

Of more than academic interest was a parallel, but independent, study conducted by Boeing on the first 60 flights of their BOMARC missile, an unmanned, single-string, ramjet-powered interceptor. The authors collaborated on the ground rules for the study but not on the actual analysis. The similarity of the results [a virtually identical bar chart] is striking, especially when considering that the X-15 study was projecting from a piloted, redundant design to an unpiloted, nonredundant design, and the BOMARC study was the reverse...

("X-15 Contributions to the X-30", Robert G. Hoey, pp 103-121.)

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

#### Fly-by-wire SAAB

<Brian.Randell@newcastle.ac.uk> Thu, 12 Mar 92 11:03:25 GMT

The following article appeared in the Wednesday 11 March 1992 issue of The Independent, a (quality) national paper here in the UK. It is quoted in its entirety, except for the umlaut over the "a" in "Branneby", without permission. (On a recent flight I took, as we taxied to the terminal after touch down, the pilot thanked the passengers for flying with the particular airline, and pointedly remarked that the safest part of our journey had just been completed

:-)

Brian Randell

=============

COMPUTER SYSTEMS DEVELOPED FOR AIRCRAFT ARE BEING ADAPTED FOR USE ON THE ROAD.

Susan Watts reports

CAR FIRM FORGES AHEAD WITH DRIVE-BY-WIRE PROTOTYPE

SAAB, the Swedish car maker, seems untouched by recent controversy over fly-by-wire aircraft, and is pressing ahead with plans for a drive-by-wire car. Fly-by-wire aircraft rely on software controls to a far greater extent than conventional aircraft. Three fatal crashes of the A320 aircraft have raised fears over the safety of such systems, and how easy they are to fly.

Saab's parent, the Saab Scania Group, has experience of computer-controlled transport, having built the Grippen fly-by-wire fighter aircraft. Its automotive engineers have produced a prototype computer-controlled car. The Independent took a brief test drive yesterday. The car felt very smooth to drive, and remarkably easy to handle, although we did only a few miles an hour.

Saab concedes that safety fears could be one of the biggest obstacles to selling such a radical change in car design. But it predicts that by the time the car is in production people will be more confident about computer-controlled transport.

There is no steering wheel, but a joystick to one side of the driver. There is no mechanical link between the joystick and the wheels a computer intervenes to control and optimise the hydraulic steering. The car has a back-up control system that performs the same basic tasks as the computer, but uses traditional electronics. This is ready to switch into action if any part of the computer fails, or the driver hits an emergency "stop" button. To steer, the driver turns the joystick from side to side, and the computer translates this into wheel movement. The car senses the driver's movements on the joystick, translates these into the optimum wheel angles and feeds back information to the driver by altering the response felt through the joystick. At low speeds, for manoeuvres such as parking, a small movement of the joystick produces a large change in direction of the wheels. At higher speeds this relationship changes, so a larger movement of the joystick is needed to shift the wheels.

The prototype has a computer keyboard and flat-screen display in the passenger seat, so the driver can modify the software to change the "feel" of the joystick. Per Branneby, the Saab test engineer who heads the steer-by-wire project, said: "I can make it feel like a go-kart or an American limousine."

The idea is that driving without a steering wheel is physically safer, because you can fit an airbag where the steering wheel would be and avoid the crushing injuries often sustained by drivers in accidents.

It should also be safer because the computer and hydraulics in between the wheels and the joystick filter out "noise" from the road that would normally make the steering wheel shake and judder such as stones in the road or gusty winds.

Mr Branneby said drivers get most of the information they need to steer the car by monitoring sideways forces on their seat. In the Saab car, the computer is fed data from sensors that tell it about these forces, as well as the car's speed and acceleration. The car does not sense the environment it is in, so cannot respond automatically and change its steering to deal with a bumpy or icy road, or a skid. This is the next stage in Saab's research.

The two-litre Saab 9000 Turbo used to test the active steering has automatic gears and anti-lock brakes and a conventional accelerator, although Mr Branneby said these may eventually be linked to the central computer. He does not envisage production models of cars using steer-by-wire joysticks until 2010 or 2015, although a version with active steering applied to a conventional steering wheel may come sooner. He also said a production model would probably have two joysticks one for each arm so the driver can swap the arm in control.

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

## 🗡 Bugging ISDN

<gnu@toad.com> Fri, 13 Mar 92 07:06:38 -0800

----- Forwarded Message

Date: Thu, 12 Mar 92 19:15 GMT From: Sanford Sherizen <0003965782@mcimail.com> Subject: Corporate Strategies for Information Protection, Ethics and Privacy

As the Conference Program Director, I would like to invite readers of RISKS to attend an important upcoming executive briefing entitled

AVOIDING MANAGERIAL LIABILITY: DEVELOPING CORPORATE STRATEGIES FOR INFORMATION PROTECTION, ETHICS AND PRIVACY

Sunday evening, April 26 and all day Monday, April 27, 1992 at Bentley College, Waltham, Mass.

Sponsored by the Center for Business Ethics at Bentley College

Managers are on the hotseat. They are increasingly being given responsibilities for information protection, ethics and privacy issues. The emphasis of this briefing will be on how managers can best respond to these challenges.

Technological developments are intensifying protection, ethics and privacy as business problems. The Federal Sentencing Guidelines and other legal decisions are defining senior managers as directly responsible for developing corporate conduct rules and programs to deter organizational and employee wrongdoing. The media and public opinion are more clearly defining appropriate and inappropriate activities.

Managers need assistance to understand these complex issues and to select appropriate business policy choices. Those attending this briefing will:

Evaluate information protection, ethics and privacy issues in managerial/business terms;

Hear successful policy choices, options and tradeoffs;

Learn how to respond appropriately to these issues;

Have an opportunity to network with peers from around the nationa who are facing similar decisions.

John Poduska, a respected figure in the computer field, will give the keynote address on Sunday evening. On Monday, there will be overview presentations on technology, law, and ethics strategies. Joe Murphy, co-editor of Corporate Conduct Quarterly, will give a luncheon speech on the Federal Sentencing Guidelines. Small interactive discussion groups will be formed to evaluate scenario and to discuss specific strategies. The day will end with general sessions and idea exchanges. The fee for this exciting day-and-a-half conference will be \$300. That includes the program, a reception, all meals and informative briefing materials.

For further information, contact the Center for Business Ethics, Bentley College, 175 Forest Street, Waltham, MA 02154-4705, (617) 891-2981. Specific questions can also be sent to me by E-mail at MCI Mail 396-5782.

Sanford Sherizen, Data Security Systems, Natick, Mass.

#### 🗡 Backlog

RISKS Forum <risks@csl.sri.com> Mon, 16 Mar 92 14:45:03 PST

The backlog is excessive, I was overly busy, and our computer systems suffered several outages at times that might otherwise have permitted me to put out another issue. Sorry for the delay. However, the backlog is mostly second-and third-order stuff, which may or may not get included in the future, depending. During the previous week I think I was too permissive, so I am likely to swing back the other way for a while. Thanks for your patience. PGN

#### Mice do roar! was re: Mouse restrictions on American Airlines

Scott Colwell <scott@labtam.labtam.oz.au> Wed, 11 Mar 92 13:46:09 +1000

[John Bartlett tells of his encounter with a flight attendant over the regulations restricting the use of external mice (mouses?)]

Just 2 weeks ago I attended the RFI emission testing of our one of our X terminals and where did the major emission come from? If you guessed the mouse then you're right.

A major source of emissions from equipment in the VHF band is the cables. They act as antennas, radiating whatever noise is on the circuits that connect to them. Mouse cables are often the worst offender since they are rarely shielded.

So there is a very definite technological basis for this regulation but perhaps the problem could be covered better. I would prefer to see the regulation require that the mouse have FCC class B or CISPR 22 class B approval if this reduces the RFI levels to suitable levels. If this does not remove the problem then a new more stringent standard needs to be developed.

But if a lower level of RFI is required, then why don't the laptops themselves interfere with navigation instruments ? It is risky in the least to assume that removing the mouse will turn an FCC class B laptop into a significantly quieter device.

(By the way, leaving the mouse plugged in will most likely still radiate

regardless of whether it is used or not.)

Scott Colwell Labtam Australia Pty. Ltd. net: scott@labtam.labtam.oz.au Melbourne, Australia phone: +61-3-587-1444

## Ke: Mouse restrictions on American Airlines (Frankston, <u>RISKS-13.26</u>)

Rob Warnock <rpw3@rigden.wpd.sgi.com> Mon, 9 Mar 92 08:37:06 GMT

But there very well may be [a difference]. I have seen cases in which \*significant\* interference was radiated from an external mouse cable [into a nearly audio input, as it happened]. All it takes is the airline running into one such case, and they will tend to ban the entire class of device. Such is the reasoning which [correctly, in my view] led to the banning quite a few years ago of "pin printers" on airplanes. When I would ask if I could use my portable computer [back then it was required that you ask], the answer was always, "Yes, but not if it has a printer on it." Seems the output drivers for the pins radiated a lot. These days, the boogyman de jure may be external mice. I don't doubt that they've seen at least one such case...

Rob Warnock, MS-9U/510 Silicon Graphics, Inc., 2011 N. Shoreline Blvd., Mountain View, CA 94039-7311 (415)335-1673 rpw3@sgi.com

## Ke: Mouse restrictions on American Airlines (Frankston, <u>RISKS-13.26</u>)

Usenet Newsmaster, good@pixar.com <news@pixar.com> Mon, 9 Mar 92 01:29:08 PST

There is a potentially big difference. The wire leading to the mouse could make a wonderful transmitting antenna through which the RF soup in your shielded computer might leak out. Remember that it is only by the airline's good graces that you're allowed to use the computer at all. Electronic devices such as computers, radios and TV's are all potential sources of RF interference. Only radios and TVs are typically banned because of the specific way in which they interfere with VOR recievers. My guess is that American has traced some interference to the use of a mouse. Other airlines can't be far behind.

Let's find ways to cooperate before the NTSB has to put the use of a mouse as a probable cause for an accident. I'd rather know that the aircraft's navigation equipment is working without interference than use a mouse. But then I \*am\* typing this on a PowerBook.

--Craig

## 🗡 Risky humour

Brian Rossmajer <bwrossma@descartes.waterloo.edu> Sun, 8 Mar 92 14:26:05 EST Several people have mentioned that mouse cords can affect aircraft instrumentation. What are the known effects of, say, a six-foot mouse cord on the altimeter of an Airbus 320?

bwrossmajer@descartes.waterloo.edu (Brian W. Rossmajer)

#### 🗡 Antennas

<Bob\_Frankston@frankston.std.com> Mon 9 Mar 1992 09:15 -0500

To all of you pointing out that a mouse cord can act as an antenna. Yes, I know it is possible, but was just passing on another's comment and didn't want to confuse the issue by adding my own editorial commentary.

While I realize that air safety is a crucial issue, the airlines should have some of the burden of establishing a rational policy . If there is a significant danger from mouse cords, then they should explain and substantiate it. Otherwise, I'll confine all my flying to red-eyes since I'll have to treat airplanes as being good only for sleeping. If I'm awake, who knows what damage I'd do.

On a slightly more serious note, are the electronics in airplane's all that fragile? Is a laptop computer really worse than a thunderstorm? Are camcorders allowed? Handheld LCD games? Flashbulbs? As our electronics become more mobile, the airlines have an opportunity to be compete the for the best environment. Some will provide travellers with better ways to work while travelling while others will offer an electronics-free environment for relaxation. Of course, the nonE flights would mean you can't even write a letter home without learning how to write with a pen (remember those?)

## ✓ Email registration for IEEE SRSP [Program from <u>RISKS-13.05</u> repeated]

Elizabeth Luntzel <luntzel@csl.sri.com> Mon, 16 Mar 92 14:47:01 -0800

[This is an annual meeting of the security research community, for serious security folks, and is usually an outstanding gathering. Space limited, register early. See you there? PGN]

1992 SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, 4-6 May 1992 REGISTRATION INFORMATION

^^^^

7:00am: Registration opens8:45--9:00: Welcoming Remarks: Deborah Cooper, John McLean

9:00--10:30: DISTRIBUTED SYSTEMS: John Rushby, Session Chair
9:00-- 9:30: On Inter-Realm Authentication in Large Distributed Systems Virgil Gligor, Shyh-Wei Luan, Joseph Pato

9:30--10:00: Integrating Security in a Group Oriented Distributed System Michael Reiter, Kenneth Birman, Li Gong 10:00--10:30: Authorization in Distributed Systems: A Formal Approach Thomas Woo, Simon Lam 11:00--12:00: COVERT CHANNELS: Tom Berson, Session Chair 11:00--11:30: Lattice Scheduling and Covert Channels Wei-Ming Hu 11:30--12:00: The Influence of Delay Upon an Idealized Channel's Bandwidth Ira Moskowitz, Allen Miller 12:00--2:00: LUNCH (included in registration) 2:00--3:00: INTEGRITY: Dick Kemmerer, Session Chair Marshall Abrams, Ed Amoroso, Teresa Lunt, James Williams 3:30--5:00: CRYPTOGRAPHIC PROTOCOLS: Dan Nessett, Session Chair 3:30--4:00: Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks Steven Bellovin, Michael Merritt 4:00--4:30 On Message Integrity in Cryptographic Protocols Stuart Stubblebine, Virgil Gligor 4:30--5:00: Roles in Cryptographic Protocols **Einar Snekkenes** 5:30 RECEPTION (good food and drinks, on the house) 8:00: POSTER SESSIONS TUESDAY 9:00--10:30: SECURITY MODELS: George Dinolt, Session Chair 9:00-- 9:30: The Typed Access Matrix Model Ravi Sandhu 9:30--10:00: A Resource Allocation Model for Denial of Service Jonathan Millen 10:00--10:30: Non-Monotonic Transformation of Access Rights Ravi Sandhu, Gurpreet Suri 11:00--12:00: INFORMATION FLOW: Dale Johnson, Session Chair 11:00--11:30 A Logical Approach to Multilevel Security of Probabilistic Systems James Gray, Paul Syverson 11:30--12:00 Using Traces of Procedure Calls to Reason About Composability **Catherine Meadows** 12:00--2:00: LUNCH (included in registration) 2:00--3:00: INVITED SPEAKER: John McLean, Session Chair 2:00--3:00 Security in Distributed Systems **Butler Lampson** 

3:30--5:00: CONCURRENCY CONTROL: Tom Haigh, Session Chair 3:30--4:00: A Multilevel Transaction Problem for Multilevel Secure Database Systems and Its Solution for the Replicated Architecture Oliver Costich, John McDermott 4:00--4:30: A Two Snapshot Algorithm for Concurrency Control Algorithm in Secure Multi-Level Databases Paul Ammann, Frank Jaeckle, Sushil Jajodia 4:30--5:00: Alternative Correctness Criteria for Concurrent Execution of Transactions in Multilevel Secure Database Systems Sushil Jajodia, Vijayalakshmi Atluri 5:00: MEETING OF THE IEEE Technical Committee on Security and Privacy 8:00: POSTER SESSIONS WEDNESDAY 9:00--10:30: SYSTEMS: Tanya Korelsky, Session Chair 9:00-- 9:30: Evolution of a Trusted B3 Window System Prototype Jeremy Epstein, John McHugh, Rita Pascale, Charles Martin, Douglas Rothnie, Hilarie Orman, Ann Marmor-Squires, Martha Branstad, Bonnie Danner 9:30--10:00: A Neural Network Component For An Intrusion Detection System Herve Debar, Monique Becker, Didier Siboni 10:00--10:30: An Optimal Solution to the Secure Reader Writer Problem Glenn Benson 11:00--12:00: DATABASE SECURITY: John Dobson, Session Chair 11:00--11:30: Security for Object-Oriented Database Systems Jonathan Millen, Teresa Lunt 11:30---12:00 A Natural Decomposition of Multi-level Relations Frederic Cuppens, Kioumars Yazdanian 12:00--12:15: AWARDS 12:15: SYMPOSIUM ADJOURNS ^^^^ ADVANCE (Mar/9/92 TO Mar/23/92) MEMBER \$230 NONMEMBER \$290 STUDENT \$ 50 LATE (Mar/24/92 TO Apr/10/92) MEMBER \$280 NONMEMBER \$360 STUDENT \$ 50 Since payment must be in US dollars only, please WIRE FEE to Account Name: 1992 SYMP on RESRCH SEC & PRIVACY

Bank and Address: Home Savings of America 1800 North Sepulveda Boulevard Manhattan Beach, CA 90266-9977 Bank Routing Number: 322070006 Bank Account Number: 1369041221

AND fax a copy of the wiring information to Liz Luntzel, 1 415 859-2844, so we know you've paid.

^^^^

You may email the following information to me, luntzel@csl.sri.com, to register for the symposium.

Name: Company: Mail Stop: Street Address: City/State/Zip/Country: Phone Number:

IEEE or IEEE Computer Society Member Number:

Do You Wish to Present at a Poster Session?

Have you participated in any recent research, development, or evaluation project in computer Security? If so, please name the project and the area of computer security:

cut:^^^^^^^^^

CLAREMONT RESORT REGISTRATION: (YOU MUST REGISTER DIRECTLY WITH THE CLAREMONT.) Cut-off Date: April 2, 1992

1992 IEEE Symposium on Research in Security and Privacy, May 4-6, 1992

Check-in time is after 3:00pm; check-out is 12:00 noon

SINGLE: DOUBLE: (2 persons/1 bed) DOUBLE DOUBLE (2 persons/2 beds)

All reservations must be accompanied by an advance deposit or credit card guarantee. You may cancel your individual reservations up to 72 hours prior to arrival, after which your deposit becomes nonrefundable. The telephone number of the hotel is: (415)843-3000

To reserve Oakland Airport Transportation, please call 24 hours in advance to (415)843-3000, x133.

Group Rates: \$91 Single \$103 Double

Name: (sharing with):

Company/Group:

Street Address:

City/State/Zip/Country::

I WILL ARRIVE ON (DAY) \_\_\_\_\_ (DATE):\_\_\_\_ I WILL DEPART ON (DAY) \_\_\_\_\_ (DATE):\_\_\_\_

I WILL GUARANTEE MY RESERVATION WITH:

ADVANCE DEPOSIT: \_\_\_\_\_ CREDIT CARD: \_\_\_\_\_ Type: Expiration Date:

Please mail this section of the form with your payment to: The Claremont Resort Ashby & Domingo Avenues Oakland, CA 94623-0363

cut:^^^^^^^^^

Delta Airlines, Inc., is offering special fares to the Symposium. These fares are based on Delta's published round-trip fares within the U.S. and San Juan. A 5% discount off any published fare (except group, military, government contract, Visit USA, and Delta's Canadian fares), providing all rules and conditions of the airfare are met; a 45% discount off the unrestricted Coach (Y,YN,Y1) fare. Seven days advance reservations and ticketing is required. Exceptions: Travel from Delta's Canadian cities will apply at 40% discount, and travel solely on Delta Connection Carriers will appy at a 35% discount. To take advantage of these discounts, call Delta, or have your travel agent call, at 1-800-241-6760, for reservations (8-11:00pm EST daily). Refer to file number H0575. Certain restrictions may apply and seats are limited. These discounts are available only through Delta's toll-free number.

^^^^

If you need any further information, including an on-line or FAX copy of the program, please email me. We look forward to seeing you at the Symposium!

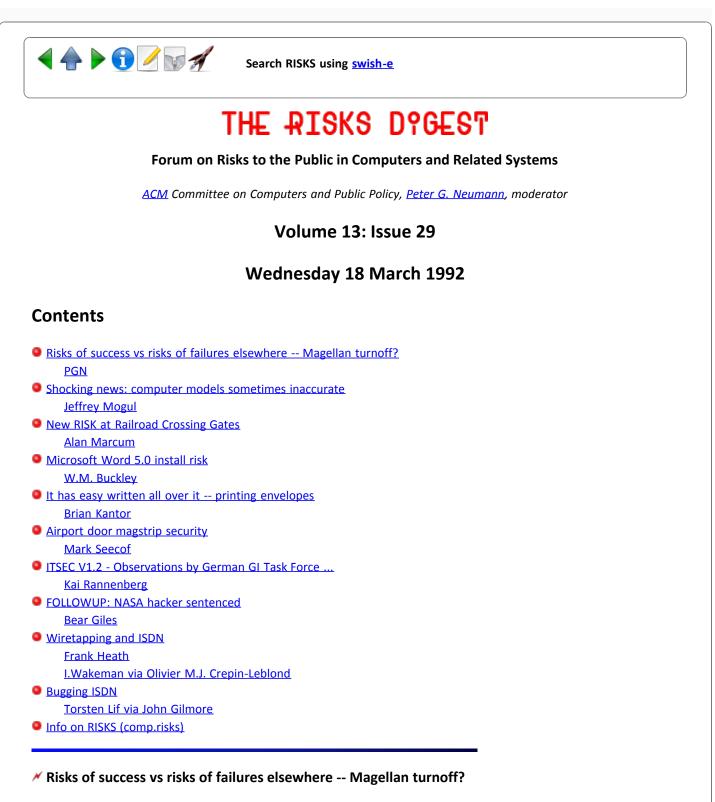
Liz Luntzel (Teresa Lunt's Assistant)

^^^^



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Tue, 17 Mar 92 9:53:49 PST

The lead item in this week's Talk of the Town (New Yorker, 16 Mar 1992, pp.31-32) is a letter reporting on NASA's plan to abandon the Magellan spacecraft (which is scientifically an enormous success and which is continuing to produce remarkable results, far beyond original expectations), in order to save a few million dollars. The letter makes a very compelling case for the incremental benefits of keeping the mission going, and concludes thusly:

Given the cost of building Magellan and getting it to Venus -- about half a billion dollars -- most of the NASA scientists think that to turn it off prematurely is penny-wise and pound-foolish. It is the loss of a kingdom -more than that, of a planet -- for want of a nail.

#### ✓ Shocking news: computer models sometimes inaccurate

Jeffrey Mogul <mogul@pa.dec.com> 18 Mar 1992 1542-PST (Wednesday)

E-470 hits new detour (Mary George, Denver Post Environment Writer, Denver Post, 13 Mar 1992, Page 2B

The E-470 Public Highway Authority clocked another delay in its race to the new Denver Airport yesterday when the company that wants to finish the \$1 billion tollway revealed it's having computer troubles.

A computer model, which seeks to forecast traffic and toll revenues, isn't yet accurate enough to satisfy state transportation officials considering a \$100 million loan for the highway, or financiers who would help bankroll 31 miles of four-lane construction, said Ed Gorman, chief executive officer of Morrison Knudsen, the company seeking to build the road.

The revenue forecasts and financial plans now have been delayed since February. The delay is costing the company about \$250,000 a month.

[The rest of the article is about high finance, except for this last sentence:]

About 3,275 drivers used the existing E-470 segment daily last month, not enough to pay for tollway operations.

[What I found interesting about this story was that the company was thwarted not because its model didn't produce the result that the financial backers wanted, but because they didn't trust the result. (At least, that's the implication of the article; perhaps the model was declared "inaccurate" simply because it doesn't forecast enough revenue.) Are public officials and financiers finally realizing that just because a computer model says something doesn't mean that it is so? -Jeff Mogul]

[P.S.: By the way, if they charged each of those 3275 drivers \$2 each day, it would take 418 years to pay back the \$1 billion construction cost (excluding several quintillion dollars of interest expense). JM]

## New RISK at Railroad Crossing Gates

Alan M. Marcum - TS <Alan\_Marcum@NeXT.COM> Wed, 11 Mar 92 09:46:02 PST

This morning, while on my way to deliver my 19 month old son to the babysitter,

the railroad crossing gate closed. It opened shortly after that, with no train having passed.

Now, this sounds like a completely benign failure mode, yes? Not if you have a 19 month old who LOVES trains in the car! Joshua sure got upset when no train followed the gate's closing...

Alan M. Marcum, NeXT Technical Support amm@NeXT.COM

# Microsoft Word 5.0 install risk

<buckley@regulus.llnl.gov> Tue, 17 Mar 92 11:37:47 PST

An increasing number of software manufacturers are encountering problems with viral infections of their products. It is interesting that in an environment where manufacturers and users are becoming more cautious, that the installation procedure for Microsoft Word 5.0 includes directions to remove any virus protection from your system before proceeding with the installation.

W.M. Buckley - Applications Systems Division - LLNL (510)423-4581 buckley@Ill-winken.llnl.gov

# It has easy written all over it -- printing envelopes

Brian Kantor <brian@UCSD.EDU> Wed, 18 Mar 92 07:20:58 -0800

On page 23 of the latest [April 1992] issue of Scientific American is a two-page spread from Microsoft touting their "Word for Windows" product, including a tag pointing out how easy it is to print envelopes: "Easy. We mean REAL easy. There's an envelope command right on the screen that addresses and prints automatically."

And indeed, the envelope shown resting on top of the sample letter in the photo is nicely addressed, with the printing all lined up and centered.

But the address on the letter and the envelope differ - some of the digits in the Zip Code got scrambled between the address on the letter and the address on the envelope.

[And neither Zip Code is proper for San Diego, which is the city shown in the address. One is in Los Angeles, and I think the other is much further north.]

What's the Risk? Financial. If you're going to advertise a feature, you should at least make it look like it works. One can't help but wonder how much such an error affects sales.

- Brian

# irport door magstrip security

Mark Seecof <marks@capnet.latimes.com> Tue, 17 Mar 92 13:28:13 -0800

In <u>RISKS 13.28</u> Brian Randell reported a series of bank ATM robberies involving forged magstripe cards.

On page B3 of the 17 March '92 Los Angeles Times an article by Hugo Martin headlined "Security Upgraded At Airport" reports that Burbank airport (one of L.A.'s smaller airports) will install an \$83,000 electronic locking system to meet FAA requirements for more stringent control of access to non-public areas. The system will replace current key and combination locks. Airport employees will get badges with magstripes. Doors will be unlocked by a computer when authorized personnel swipe their cards through readers adjacent to the doors. The system will allow for giving or revoking authorization on short notice, and for conditioning authorization on time of day (or week, etc). "The new system also records each employee's use of a door, allowing airport officials to determine which employees were present in a secured area at a given time."

Risks? The usual from (IMHO) insufficiently thought-out systems. The system will not, in fact, provide a good record of which people were in a secured area at a given time, because the doors aren't being changed and people can pass through them without authorization or recordation when they're opened by other people. Also, it's easy to duplicate the magstripes on the cards. A photo with the story suggests that a combination (passcode) could be required along with the card (it shows a card reader with a keypad) but the story doesn't mention if this is done.

Mark Seecof Publishing Systems Department, Los Angeles Times

## ITSEC V1.2 - Observations by German GI Task Force ...

Kai Rannenberg <kara@cs.tu-berlin.de> Thu, 19 Mar 1992 01:54:42 +0100

Statement of Observations concerning the Information Technology Security Evaluation Criteria (ITSEC) V1.2

The Information Technology Security Evaluation Criteria (ITSEC) are the result of an initiative driven by the Commission of the European Communities. Their current version 1.2 from June 1991 is the basis for the evaluation of secure IT systems in the EC member countries for at least until 1993.

Although the ITSEC are quite advanced compared to the TCSEC (Orange Book) and there have been discussions on V1.0 and V1.1, a lot of several critical points remained in V1.2, especially aspects of possible functionalities and assurance methods.

Therefore the Data Protection and Data Security Task Force of the German Society for Informatics (GI) decided to issue and publish a "Statement of observations concerning the ITSEC V1.2". Observations, criticism and proposals concentrate on the following issues:

- (1) Title and Scope of ITSEC
- (2) Functionality
- (3) Assurance Effectiveness
- (4) Assurance Correctness
- (5) Post-Evaluation Problems
- (6) Development and Discussion of the ITSEC

The full text has been posted to alt.security, misc.security and comp.security.

Kai Rannenberg Technische Universitaet Berlin Informatics Department Sekretariat FR 5-10, Franklinstr. 28/29, D-W-1000 Berlin 10, Germany kara@cs.tu-berlin.de Phone: (+49 30) 314-73499 Fax: (+49 30) 314-24891

[It is also available for anonymous FTP from CRVAX.SRI.COM with RISKS-13.ITSEC as its file name. Important for security-minded folks. The ITSEC is good stuff. PGN]

# *FOLLOWUP*: NASA hacker sentenced

Bear Giles <bear@tigger.cs.colorado.edu> Tue, 17 Mar 1992 13:05:09 -0700

From the 17 March 1992 \_Rocky Mountain News\_:

Hacker ordered to get mental help (Reuter)

A computer hacker who pleaded guilty Monday to breaking into NASA computer systems as ordered to undergo mental health treatment and not use computers without permission from a probation officer. Richard Wittman, 24, of Lakewood [Colorado] was sentenced to three years probation by Denver U.S. Distrcit Judge Sherman Finesilver in a rare prosecution for breaking into a computer system. Wittman pleaded guilty last fall to one count of breaking into a National Aeronautics and Space Administration computer. Prosecutors said Wittman had spent four years trying to get into computer systems. In a plea bargain, Wittman admitted gaining access to NASA's computer via a malfunction in a bulletin board service.

# Wiretapping of future communication networks

"Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.ic.ac.uk> Thu, 12 Mar 92 0:38 BST

The following couple of articles were sent to the ISDN discussion list. I have briefly commented at the end. (very briefly) OCL.

\_\_\_\_\_

Date: Tue, 10 Mar 92 09:32:56 PST From: heath@com.CMC (Frank Heath) Subject: Wiretapping and ISDN Sender: isdn-request%com.Prime.List@com.Prime.Relay

From the LA Times Saturday, March 7,1992 FBI Fear Phone Advances Will Hamper Wiretapping

Washington- The FBI, contending that rapidly developing telecommunications technology is hampering the vital tool of wiretapping, proposed legislation Friday that would require the industry to ensure that improvements do not interfere with the ability to secretly record conversations.

It also proposed that consumers pick up the cost of changing current wiretapping equipment to keep pace with new technology.

If the problem is not solved, "terrorists, violent criminals, kidnapers, drug cartels and other criminal organizations will be able to carry out their illegal activities using the telecommunications system without detection." FBI Director William S. Sessions said. [...]

At issue is the rapid move toward digital telephone communications and fiber-optic systems in which thousands of conversations can be carried by filaments roughly the size of a strand of human hair.

William A. Bayse, assistant FBI director for technical services, and other FBI officals contend that the transmission of hundreds and sometimes thousands of digital conversations over a single link prevents current wiretapping technology from isolating conversations for recording as required under the 1968 federal wiretap law. [...]

Other FBI offical said the expense could be passed on to telephone users at a cost of "probably less than 20 cents an average per month." [...]

FBI officals maintained, however, that they already have encountered difficulties in recording digitally transmitted conversations, now used by about 10% of the nations phones. They declined, however, to give any examples of such difficulties.

[Well folks, we may have finally discovered the long awaited "Killer ISDN Application", drug dealing! ;-)

On a more serious note is the FBI's technology that broken, that it can't deal with multiplexed transmission? You would think the NSA has sufficent technology to do it. I don't know of ISDN phones that come with built in scramblers, although it would be pretty easy to do. I don't think this is what they are talking about here.

Particulairly galling is we are all going to be changed 20 cents a month to support big brother type intursions.

This sort of legislation can't help but to slow ISDN's already glacial deployment.

For the ASI types what we need now is a new session block,

Circuit Switched Voice, Secure(except where prohibited by law).

Frank S. Heath, CMC.COM My views not CMC's or Rockwell's. ]

[And here is a followup article - OCL]

Date: Tue, 10 Mar 92 17:54:13 +0000 From: I.Wakeman@uk.ac.ucl.cs Sender: isdn-request <isdn-request%com.prime.list@com.prime.relay>

I find it strange that the FBI should be tapping into lines directly (I saw an old Cagney and Lacey last night which had them sitting in a basement with a breakout box and a tape-recorder - definitive proof of the obsolescence of US police equipement). Here in the UK, there is this persistent rumour that our digital exchange has the most advance security facilities in the world, allowing tapping of a conversation at the switch rather than on the wire. This means our police don't have to get their hands dirty, assuming that the Home Secretary gives permission, and all they need to do is attach a tape-recorder (or tape drive) to a port at the exchange.

Does this mean we can expect the sales of System X to take off in the US, as long as the FBI give their backing? Or are the FBI forbidden to attach to the switch?

cheers, ian

[One of the forthcoming set of RISKS related to future telecommunication systems. I'm currently working on Broadband ISDN, and believe me, when that will be implemented, I doubt that the FBI will even bother about monitoring lines due to the excess amount of information being transmitted. Olivier M.J. Crepin-Leblond, Imperial College London, UK.]

## Bugging ISDN

Torsten Lif <etxorst@eos.ericsson.se> Fri, 13 Mar 1992 09:54:50 GMT

The recent thread on ISDN and bugging reminded me of an interesting issue.

Some years ago I worked in Ericsson's effort on designing ISDN phones. One of the features we implemented was that in order to faciliate testing, the exchange could send signals to set up loops in the terminals (this is fairly standard) and to leave an "open end" in case deeper testing was ever needed, a mechanism for reading or writing any data address on the terminals internal system bus was provided. In theory, a piece of code could then be added byte by byte to the RAM of the terminal and a patch jump applied to link it in. Not that I think anybody would be foolhardy enough to actually do it, but in theory it would be possible.

But one morning in a coffee-break brainstorm-session we started speculating on what COULD be done if a feature like this were abused (say, by the FBI) and we

realized that since all the control ports of the phone were regular bus devices, anybody who knew the address to the proper latch (easy to read if you got hold of the system description documents), could send the instructions to activate the microphone and connect it to a B-channel without going through all the layer-3 protocol stuff or the phone's internal program. Just a couple of "POKE"s and presto, the room is bugged. This would be more devious than the "normal" kind of bugging where a line is tapped, since it would take place when there's no phone call going on.

So as a collective act of civil disobedience the HW and SW designers got together and put in an extra HW "AND" gate in a strategic location so that the bitstream from the codec to the S-interface was choked unless either the receiver was (hardware) off-hook or the "hands-free" indicator LED was turned on. This meant that the SW had to set two latches to connect the phone to the line but, hey, that's what macros are for... At least, if anybody were to try and turn the phone on for bugging purposes, they would have to turn on the LED on the front. Hopefully this would be conspicious enough to alert anybody in the room.

Of course, this didn't prevent bugging of a phone call, but that's impossible to guard from without encryptation anyway. ALL exchanges have supervision devices that can be (ab)used to listen in on conversations. Telecom manufacturers selling to certain countries routinely get orders for far more supervision equipment than would normally be needed. Why is not too hard to guess.

The upshot of this is that when I read the discussions about FBI's fear of new technology, I remembered what we did to deliberately prevent something akin to what they want legislation to force designers to give them. Does this mean that I'm now "Persona Non Grata" in the US? :-)

Any others out there who can think of similar "features" of the new digital technologies? Are we (the guys who then worked at Ellemtel) the only ones to have thought of it and tried to prevent it? Are there any others on the list/net who have worked in the field and have stories to share?

Torsten Lif Ericsson Telecom AB, EO/ETX/TX/ZD S-126 25 STOCKHOLM, SWEDEN Phone: +46 8 719 4881

## *K* CFP Workshop on Feature Interactions in Telecommunications Systems

Nancy Griffeth <nancyg@banshee..bellcore.com> Wed, 18 Mar 92 20:15:09 GMT

**Call For Participation** 

INTERNATIONAL WORKSHOP ON FEATURE INTERACTIONS IN TELECOMMUNICATIONS SOFTWARE SYSTEMS

St. Petersburg, Florida, USA, December 3-4, 1992

#### DESCRIPTION

This workshop is planned to encourage researchers from a variety of computer science specialties (software engineering, protocol engineering, distributed artificial intelligence, formal techniques, and distributed systems, among others) to apply their techniques to the feature interaction problem that arises in building telecommunications software systems.

The feature interaction problem has been a major obstacle to the rapid deployment of new telephone services. Telecommunications software is huge, real-time, and distributed; adding new features to a telecommunication system, like adding new functionalities to any large software system, can be very difficult. Each new feature may interact with many existing features, causing customer annoyance or total system breakdown. Traditionally, interactions were detected and resolved on a feature by feature basis by experts who are knowledgeable on all existing features. As the number of features grows to satisfy diverse needs of customers, managing feature interactions in a single administrative domain is approaching incomprehensible complexity. In a future marketplace where features deployed in the network may be developed by different operating companies and their associated vendors, the traditional approach is no longer feasible. How to detect, resolve, or even prevent the occurrence of feature interactions in an open network becomes an important research issue.

The feature interaction problem is not unique to telecommunications software; similar problems are encountered in any long-lived software system that requires frequent changes and additions to its functionality. Techniques in many related areas appear to be applicable to the management of feature interactions. Software methodologies for extensibility and compatibility, for example, could be useful for providing a structured design that can prevent many feature interactions from occurring. Formal specification, verification, and testing techniques, being widely used in protocol engineering and software engineering, contribute a lot to the detection of interactions. Several causes of the problem, such as aliasing, timing, and the distribution of software components, are similar to issues in distributed systems. Cooperative problem solving, a promising approach for resolving interactions at run time, resembles distributed planning and resolution of conflicting subgoals among multiple agents in the area of distributed artificial intelligence. This workshop aims to provide an opportunity for participants to share ideas and experiences in their respective fields, and to apply their expertise to the feature interaction problem.

We welcome papers on preventing, detecting, and/or resolving feature interactions using either analytical or structural approaches. Submissions are encouraged in (but are not limited to) the following topic areas:

- Classification of feature interactions.
- Modelling, reasoning, and testing techniques for detecting feature interactions.
- Software platforms and architectures for preventing or resolving feature interactions.
- Tools and methodologies for promoting software compatibility and extensibility.

# Environments and automated tools for related problems in other software systems. FORMAT

We hope to promote a dialogue among researchers in various related areas, as well as the designers and builders of telecommunications software. To this end, the workshop will have sessions for paper presentations, including relatively long discussion periods. Panel discussions and a short tutorial on issues in the feature interaction problem are being organized.

#### ATTENDANCE

Workshop attendance will be limited to 75 people. Attendance will be by invitation only. Prospective attendees are asked to submit either a paper (maximum 5000 words) or a single page description of their interests and how they relate to the workshop. About 16--20 of the attendees will be asked to present talks. We will strive for an equal mix of theoretical results and practical experiences. A set of working notes will be provided at the workshop. Papers with the highest quality will be considered for publication in a special issue or section of a research journal.

#### SUBMISSIONS

Please send five copies of your full original paper or interest description to: Nancy Griffeth Bellcore, MRE 2L-237 445 South Street Morristown, NJ 07962-1910, USA E-mail: nancyg@thumper.bellcore.com Tel: (201) 829-4538 Fax: (201) 829-5889

#### IMPORTANT DATES

June 1992: Submission of contributions.
 August 1992: Notification of acceptance.
 September 1992: Submission of camera-ready versions.

## WORKSHOP CO-CHAIRPERSONS

Nancy Griffeth (Bellcore, USA) Yow-Jian Lin (Bellcore, USA)

#### PROGRAM COMMITTEE

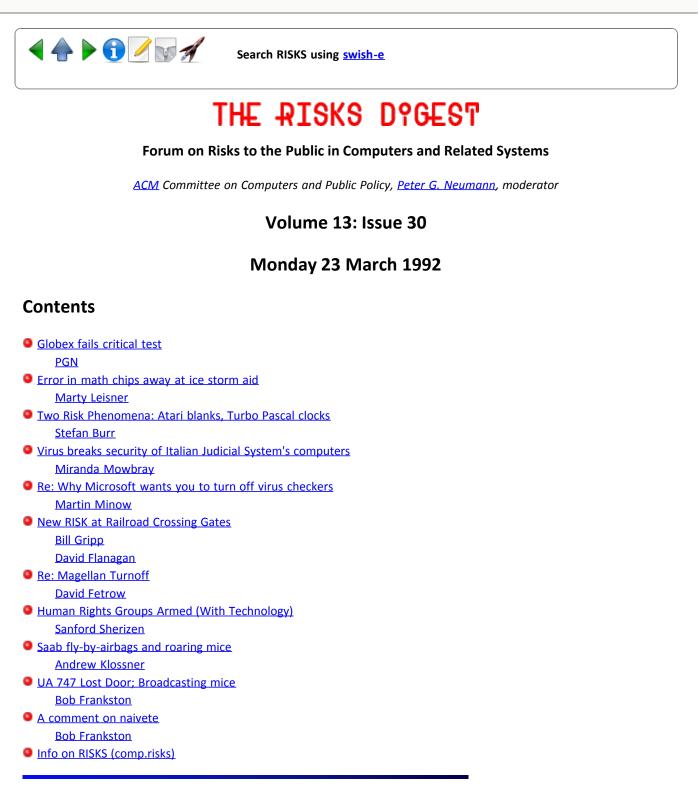
chair: Hugo Velthuijsen (PTT, The Netherlands)

E. Jane Cameron (Bellcore, USA) Steven Harris (BNR, Canada) Gerard J. Holzmann (AT&T Bell Laboratories, USA) Michael Huhns (MCC, USA) Luigi Logrippo (University of Ottawa, Canada) Harm Mulder (PTT, The Netherlands) Jan-Olof Nordenstam (ELLEMTEL, Sweden) David Notkin (University of Washington, USA) Akihiro Shimizu (NTT, Japan) Yasushi Wakahara (KDD R&D Laboratories, Japan) Pamela Zave (AT&T Bell Laboratories, USA)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# ✓ Globex fails critical test

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 20 Mar 92 10:47:36 PST

Globex is an electronic trading system being developed by Chicago's futures exchanges and Reuters PLC, using a 30-MIPS DEC 9420 computer at Reuters' U.S. headquarters on Long Island. The development is behind schedule, having experienced repeated delays in the past two years. A previous test in January handled 30,000 mock trades successfully. The latest field test on 3 Mar 1992 (with key stations in NY, Chicago, Paris and London) aborted after only ten minutes:

The system detected a condition in which the data ... in one of the 250 key stations was different from what the host computer thought it should be, and when that occurs, the system is designed to shut down.

[Source: Chicago Tribute, 5 Mar 1992, Section 3, article by William B. Crawford Jr., contributed by Robert V. Binder, starkly abstracted by PGN]

The article includes the hopes for the system, the doubts expressed by others, and the impact the failed test had -- deferring a vote on a master agreement governing the partnership, and postponing the intended unveiling, previously scheduled for April.

## ✓ Error in math chips away at ice storm aid (Rochester paper)

Marty Leisner x76704 siena <leisner%johnker.henr801@xerox.com> Sat, 21 Mar 1992 21:47:18 GMT

In today's Democrat and Chronicle, they had a headline "Error in math chips away at ice storm aid" (in Rochester, New York they had an ice storm last year). This was for the Town of Irondequoit (a neighbor of Rochester).

They got some Federal Disaster Relief for this. The Federal government earlier promised 2.7 million dollars. They really got 1.38 million.

The conclusion was "what nobody realized at the time, officials say now, is that the total reflects a computer keypunch error."

When I first read the headline, I thought they had a bogus math chip ;-)

marty leisner.henr801c@xerox.com Member of the League for Programming Freedom (You get what you pay for -- except in software)

## M Two Risk Phenomena: Atari blanks, Turbo Pascal clocks

<CSCSAB@ccnyvme.bitnet> Wed, 18 Mar 92 22:15 EST

I know of two interesting phenomena that relate to two of your CACM Inside Risks columns. A full discussion of either would take quite a bit of time to write down in full, or (probably easier) a phone call. Therefore, I'm just going to give you a brief description of each [...].

The first is an example of a somewhat annoying computer pun, relating to your 9/90 column. This concerns Atari 8-bit computers, which were way ahead of their time, and still are to some extent. (I still use one for some tasks, although I have a much fancier computer now.) In Atari Basic, the prompt is

READY. For a long time, I noticed occasional peculiar behavior, and I could do some experiments to recall exactly the form it took. Anyway, I finally noticed that when I moved the cursor to such a prompt and hit the return key, no error message occurred. (The Atari has a full-screen editor.) I thought about this, and finally realized that the interpreter was reading this as READ Y. Just as in Fortran (except Fortran 90), blanks are irrelevant, so the prompt was treated as an immediate command. I don't think this usually caused real trouble, but it could do so if my program had a variable named Y.

The second phenomenon relates (at least partially) to your column on clocks (1/91). This one you very likely were aware of already. I was having my students do timing tests on programs on IBMs and clones. This is painful enough, just because of the absurd rate of ticks (18/sec.), but further problems are caused by the fact that the data (hours, minutes, seconds and hundredths of seconds) is in unsigned integer, 1-byte form. We were using Turbo Pascal, which is generally a useful implementation. However, this language has five (or six if the coprocessor is present or being simulated) integer types, of which three are signed and two are unsigned, and all may be freely mixed. This causes many typing problems, worse than any built into Fortran. The basic problems come from the fact that when you subtract unsigned integers, if the result is negative, the computed value becomes a positive integer, usually a large one. We found several different ways to get crazy output, including some ways that the error would not be a power of two.

-- Stefan Burr (201)-267-0137 (home) and (212)-650-6172 (work)

#### Virus breaks security of Italian Judicial System's computers

Miranda Mowbray <mjfm@pisa1.italy.hp.com> Mon, 23 Mar 92 10:39:23 +0100

Traces of the `Gp 1' virus have been discovered in the computers of the Court of Cassation, the Courts of Appeal, and the High Tribunal for Public Waters, in Italy. The virus was discovered by the central security office, which reports to the Presidency. Rather than destroying data, Gp 1 awards maximum security clearance to all minimum security level users. The other judicial offices are being checked for the virus.

Source: La Nazione, 22 March 1992

# re: Why Microsoft wants you to turn off virus checkers

Martin Minow <minow@ranger.enet.dec.com> Thu, 19 Mar 92 08:58:47 PST

In <u>RISKS-13.29</u>, W.M. Buckley notes that the installation instructions for Microsoft Word 5.0 instructs customers to remove virus protection before installation.

While I don't know the particulars of Microsoft's situation, I suspect there are two reasons:

- -- Virus protection programs trap certain operations that the installation procedure must perform in order to install the software. For example, Microsoft records the customer name, organization, and serial number "somewhere" in the application image. Depending on how they do this, this may look to the virus checker as if an intruder were modifying the image.
- -- Installing an application is a rather complex task (I am speaking here
  of the Macintosh, but I suppose this applies to other systems as well.)
  I am currently working on a Macintosh application and am budgeting
  about one week to write write a simple installation script for a much
  simpler product. Since virus protection software works by modifying
  the system image in some "secret" manner, debugging, documentation and
  customer support become expensive nightmares. The vendor is far better off
  putting more effort into manufacturing control and development.

In my own product, I'm faced with a similar problem: one of its functions is to create, under user control, small applications. Here, too, the documentation must warn the customer to add my application to the virus protection program's list of "trusted" programs.

Martin Minow minow@ranger.enet.dec.com

# Mew RISK at Railroad Crossing Gates (Marcum, <u>RISKS-13.29</u>)

Bill Gripp <billg@bony1.bony.com> Thu, 19 Mar 92 13:06:31 -0500

This is not necessarily a failure mode. Among the possibilities...

1) Railroad personnel were testing the crossing gate. This can be accomplished in one of many ways. The personel don't necessarily have to be immediately at the crossing.

2) Pranksters were having fun. Again they don't have to be immediately at the crossing.

3) A local freight train doing some switching moves entered the electrical block controlling the crossing activating the crossing gate. The train then stopped and reversed direction exiting the block, allowing the crossing gates to open.

I just love it when people say that something failed/broke when they really don't have any idea about what is going on.  $=8^{\circ}$ )

The REAL risk, is that these people sometimes get a lot of attention and as a result negatively effect the reputation of reliable equipment, companies, people, [fill in the blank]!

Ke: New RISK at Railroad Crossing Gates (Marcum, <u>RISKS-13.29</u>)

# David Flanagan <david@artemis.ora.com> Thu, 19 Mar 92 10:20:43 EST

Railroad crossing gates coming down when no train is coming just a "benign failure mode"? Not necessarily: I have a friend who admits that in his (much) younger days he would head down to the tracks near his house and close the gates just for fun. He reports that the drivers at the front of the lined up traffic were very reluctant to cross the tracks when the gates went up (much to the chagrin of the drivers just arriving at the end of the line). They assumed that the "failure" was that the gates went up too soon, rather than that they went down without cause.

My friend has reformed himself now, but I've learned some interesting things about railroad crossing gates. The (pedestrian) gates near my house (and presumably this is how most work) will go down when the tracks are shorted together. I have yet to take a voltmeter to them, however.

-- David Flanagan

# Ke: Magellan Turnoff

David Fetrow <fetrow@biostat.washington.edu> Wed, 18 Mar 92 22:07:16 -0800

In Volume 13 : Issue 29 "Peter G. Neumann" <neumann@csl.sri.com> notes an article over the purported plan to turn off Magellan before it fails due to a lack of funds.

I suspect something like the old Viking Fund will be set up by someone. At this funding level, simple charity might supply enough money to keep things going. It's a rather silly way to fund a probe, but not as silly as shutting down.

You may recall the Viking funds striking logo: Viking with a tin cup in it's claw.

-dave fetrow

# Human Rights Groups Armed (With Technology)

Sanford Sherizen <0003965782@mcimail.com> Fri, 20 Mar 92 15:14 GMT

Today's New York Times reports that the Lawyers Committee for Human Rights will start a campaign called Witness to provide human-rights groups around the world with hand-held video cameras, computers and fax machines. The Reebok Foundation and musician/composer Peter Gabriel contributed to the project. Mr. Gabriel said: "It's much easier for those in power to get away with murder, torture, repression and the destruction of our environment if their actions are not witnessed by the media and public."

While we have heard how technology contributed to the overthrow of the Shah and kepts the world's eyes on repression by the China's leaders, I wonder if this

effort is a legacy of the Rodney King beating by police officers in Los Angeles. The beating was videotaped and played over and over on tv, resulting in indictments and a current trail of police officers. Better that legacy than America's Favorite Videos or some other "let's video our kids hitting dad in the crotch" or "we'll act crazy and hope that we can get on tv with the tape", which is so popular on television today in the U.S.

Sanford Sherizen, Data Security Systems, Natick, MA

#### Saab fly-by-airbags and roaring mice

Andrew Klossner <andrew@frip.wv.tek.com> Fri, 20 Mar 92 13:12:24 PST

>From the Saab drive-by-wire report:

"The idea is that driving without a steering wheel is physically safer, because you can fit an airbag where the steering wheel would be and avoid the crushing injuries often sustained by drivers in accidents."

Curious. Chrysler puts air bags on the driver side but not the passenger side. They defend this by claiming that it's much harder to mount a bag on the passenger side -- without a steering column, there's no suitable place for it.

>From the roaring mouse discussion:

"I would prefer to see the regulation require that the mouse have FCC class B ..."

PC mice are unlike those in the Macintosh, Sun, or X terminal world in that they are usually sold as separate products. None of the three PC laptops that I've purchased have been offered with a mouse option (perhaps EMI problems were a consideration.) There is no opportunity to perform FCC testing of a PC laptop and mouse as a single system.

-=- Andrew Klossner (andrew@frip.wv.tek.com) (uunet!tektronix!frip.WV.TEK!andrew)

## VA 747 Lost Door; Broadcasting mice

<Bob\_Frankston@frankston.std.com> Sat 21 Mar 1992 09:43 -0500

There was small item in the New York Times earlier this week reporting on the United Airlines 747 that lost a door near Hawaii a few years ago. The report has been revised to say that the door was lost due to a problem with the control circuitry for the door and was not due to a mechanical problem. Hmm.

A final note on the broadcasting mice. I do realize that any external wire can broadcast and can interfere with some forms of communications.

# A comment on naivete

<Bob\_Frankston@frankston.std.com> Sat 21 Mar 1992 10:01 -0500

I meant to mention that my naivete itself was an example of taking technology advancement for granted. This similar to using an old tape deck and going directly from forward to reverse. Those used to mechanical systems would stop in the middle and give the tape a chance to stop. Those brought up on VCRs would assume that the machine would be smart enough to deal the mechanical problems "intelligently".

Similarly, my expectations of airline communications are affected by what I know is possible, even if it is naive knowledge.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# New XEROX FAX software

Jeremy Epstein <epstein@trwacs.fp.trw.com> Tue, 24 Mar 92 09:48:29 EST

Today's Washington Post has an article about a new Xerox software product designed to provide remote access to a PC through a FAX. Basically, you can FAX a message to your PC with instructions on what you want, and it will FAX the file(s) to a number of your choosing. If you don't have the form handy, FAXing a blank sheet of paper will cause it to FAX the blank form back to you. The target market is people who travel but don't carry everything they might possibly need...they call it a 24-hour-a-day assistant.

The product (whose name I've forgotten) is software...it works with

the hardware FAX boards you can buy.

The product sounds really neat, but the first thought that came to my mind was security. If I know that Jane Doe has this software on her PC, how will it prevent me from asking for a copy of anything on her PC? The article didn't mention any security measures to prevent an machine from attack.

I don't have any technical product information, so this may be merely an omission from the article, rather than a weakness in the product.

Jeremy Epstein, Trusted X Research Group, TRW Systems Division, Fairfax Virginia +1 703/803-4947 uunet!trwacs!epstein epstein@trwacs.fp.trw.com

## FYI: Congressional Advisory Board calls for public review

Jim Warren <autodesk!highpoint!jwarren@fernwood.mpk.ca.us> Wed, 25 Mar 92 17:16:42 PST

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD RESOLUTION #1 March 18, 1992

The Board has examined the present status of the proposed Digital Signature Standard (DSS) being undertaken by the National Institute of Standards and Technology (NIST). In view of:

- the significant public policy issues raised during the review of the proposed standard;
- (2) the increasingly pervasive use of digital technologies;
- the potential impacts upon the security of the unclassified/sensitive government community;
- (4) the relationship of the DSS to the existing NIST cryptographic security program; and
- (5) the posture of the U.S. in international commerce.

THE BOARD FINDS THAT:

(1) a national level public review of the positive and negative implications of the widespread use of public and private key cryptography is required. This national level review must involve the national security, law enforcement, government unclassified/sensitive, and commercial communities. Representatives from the private sector should include both vendors and users. In the next several months, NIST/NSA should sponsor a workshop on the widespread use of cryptography. This national review should be concluded by June 1993. (2) NIST has made significant progress in resolving the technical issues related to the proposed DSS. The Board recommends that NIST continue to seek resolution of the patent, infrastructure, and other remaining issues raised during the public comment process. The Board recognizes that much of the work, and in particular the infrastructure, are algorithmic independent and must be continued by NIST to assure timely implementation of digital signature technology within the government.

FOR: Colvin, Gallagher, Gangemi, Kuyers, Lipner, Philcox, Rand, Walker, Wills and Zeitler AGAINST: None ABSTAIN: None

Motion Unanimously Approved.

\_\_\_\_\_

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD RESOLUTION #2 March 18, 1992

The Board resolves that:

The approval of the Digital Signature Standard (DSS) by the Secretary of Commerce should be considered only upon conclusion of the national review.

The Board agrees to continue to monitor the activities involving the DSS and the proposed national review at future meetings.

FOR: Colvin, Kuyers, Lipner, Philcox, Rand, Walker, Wills, and Zeitler AGAINST: Gallagher, Gangemi ABSTAIN: None

-----

Motion Approved.

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD RESOLUTION #3 March 18, 1992

The Board resolves that:

The Board defers making a recommendation on approval of the Digital Signature Standard (DSS) pending progress on the national review.

The Board agrees to continue to monitor the activities involving the DSS and the proposed national review at future meetings.

FOR: Colvin, Gallagher, Gangemi, Kuyers, Lipner, Philcox, Rand, Walker, Wills, and ZeitlerAGAINST: NoneABSTAIN: None

Motion Unanimously Approved.

#### Ke: Microsoft and virus checkers (Martin Minow, <u>RISKS-13.30</u>)

<wex@pws.ma30.bull.com> Thu, 26 Mar 92 16:28:41 -0500

Well, having just installed Word 5.0 this week, I can tell you the reason: MSWord 5.0 installs things (fonts, mostly) directly into the System. All virus detectors I know of will at least trap/warn on this. But the Install program can't deal with these trap/warn windows appearing and grabbing control while Install is trying to read from disk.

So you have to turn off your virus protection. You may also have to reinstall other things in your system. In my case, the Word installation blew away my Personal Laserwriter print driver.

As long as I'm on the subject, MSWord 5.0 represents a significant step BACKWARD for Word, as far as I can tell. I'm seriously thinking of going back to 4.0 because the new interface is \*so\* bad.

Word 5.0 has several instances of the "the computer is doing something but doesn't tell the user" RISK. This, of course, causes users to repeat inputs, thinking nothing happened the first time. These additional inputs are buffered and applied to the next step in the process, potentially causing damage that is hard or impossible to undo.

The program is also significantly slower than version 4.0 (at least a factor of two in the tests I've done). This introduces the RISK that long-time Word users like myself will assume that the Mac is hung and begin diagnostic/repair actions which are inappropriate and cause bad effects.

There is more functionality than in 4.0, but a lot of it is "stupid" functionality in the sense that the new features duplicate existing features or do flat-out dumb things (we can discuss some other time the hilariously wrong messages their grammar checker spits out).

A shame, really. Microsoft does occasionally produce good products (Excel 2.2 has one of the best, most intuitive interfaces I've ever seen), but Word seems to get worse every odd-numbered release and only better with the even numbers.

Alan Wexelblat Bull Worldwide Information Systems Billerica, MA : (508)294-6120 wex@pws.bull.com wexelblat.chi@xerox.com

# ✓ Dumbing down new systems

Lance J. Hoffman <hoffman@seas.gwu.edu> Fri, 27 Mar 92 8:01:39 EST

The debate on (son of) S. 266 and on whether and how to "dumb down" computer technology to satisfy law enforcement needs is joined in The New York Times of Friday, March 27, 1992 with articles by William Sessions, FBI director, and Janlori Goldman, director of the privacy and technology project of the American Civil Liberties Union. RISKS readers with an interest (or stake) should read these articles carefully, and consider responding with letters to the editor of the New York Times of their own if they have anything to add. If the technical community wishes to be heard, it should speak up now. (Letters to their congressional representatives may not hurt either ;-) ). Lance Hoffman

Department of Electrical Engineering and Computer Science, The George Washington University, Washington, D. C. 20052 (202) 994-4955

# Mathematical The FBI Needs Industry's Help--OpEd in NYT

Kurt F. Sauer <ks@stat.tamu.edu> Fri, 27 Mar 92 07:54:31 CST

FBI Director William Sessions wrote an interesting op-ed piece in today's New York Times (Vol. CXLI, No. 48,918, Fri., Mar. 27, 1992, p. A15) dealing with the problems which federal law enforcement expects to encounter when placing court-ordered wiretaps on data circuits. When I read between the lines, it sounds as if Mr. Sessions doesn't want us to use data security which employs end-to-end encryption; perhaps other RISKS-DIGEST readers will draw different conclusions.

[Under the rubric "Dialogue/High-Tech Wiretaps"]

Keeping an Ear on Crime: The F.B.I. Needs Industry's Help

By William S. Sessions

Advances in telecommunications technology promise to deprive Federal, state and local law enforcement officers and the public of the incalculable benefits that can be obtained only by court-authorized wire-tapping.

Wiretapping is one of the most effective means of combating drug trafficking, organized crime, kidnapping and corruption in government. The Federal Bureau of Investigation does not want the new digital technology that is spreading across America to impair this crucial law-enforcement technique. Thus, after consulting with the telecommunications industry, members of Congress and executive branch agencies, the Justice Department has proposed legislation that is intended to preserve the ability of law enforcement officers to intercept conversations of people engaged in serious crimes.

This bill is consistent with legislation passed in 1968 after Congress debated the constitutional problem posed by the Government's need to address

both serious criminal conduct and the individual's right to privacy. Congress struck a balance by passing the Omnibus Crime Control and Safe Streets Act.

That law and later amendments created the meticulous procedure by which law enforcement officers obtain judicial authorization for electronic surveillance. Wiretaps can be used to address only the most serious criminal, sometimes violent, threats facing society. Only when a judge is satisfied that all statutory safeguards have been met and all other reasonable investigative steps have failed or will likely fail, are taps permitted.

Digital technology makes possible the simultaneous transmission of multiple conversations and other data over the same lines. The problem is that voice transmission will soon be replaced by an endless, inseparable stream of electronic emissions, making it virtually impossible to capture criminal conversations.

The Federal Bureau of Investigation is not complaining. As the telecommunications industry develops digital technology, new services such as Caller ID are becoming available to business and private customers. The new technology already has provided benefits for the F.B.I.--for example, it helped solve the bombing of Pan Am Flight 103.

But if digital technology is fully introduced with insufficient attention to public safety, the effectiveness of law enforcement officers will be greatly impaired.

As society and technology evolve, so do government's needs and responsibilities. And, yes, the burden of helping to safeguard the public often falls on those who make profits from regulated goods and services. It is reasonable for the telecommunications industry to come to the aid of law enforcement. The proposed legislation relies on it to find technical solutions that are cost effective while permitting the developement of its technology. Surely it can do both in a way that insures its competitiveness.

Indisputably, there will be financial costs associated with whatever technical solutions the private sector might develop. These costs cannot be measured only in dollars; consider the price society would pay if the ability to solve complex crimes were thwarted by an end to wiretapping. In a recent large-scale military-procurement fraud case-- which was successful because of wiretaps--the fines, restitutions, forfeitures and savings to taxpayers exceeded \$500 million.

The cost to telecommunications companies would not be so substantial as to outweigh the consequences of an inability of law enforcement to act. But if nothing is done soon, as technology advances and the digital systems become more widespread, the cost of addressing the issue down the road will undoubtedly increase dramatically.

The proposed legislation does not expand the authority of the F.B.I. or any other criminal justice agency. It simply preserves what Congress authorized in 1968--nothing more.

In recent years, Congress has expanded the Federal criminal activities for which wiretapping may be obtained. As in 1968, it must decide if law enforcement should have this invaluable tool available. I am confident that congress will again support law enforcement by approving the necessary legislation.

# Accidental stock sale: The error crept in when ...

<Bob\_Frankston@frankston.std.com>

# Fri 27 Mar 1992 14:47 -0500

Speaking of rekeying the following is from the Friday March 27, 1992 in an article about Salomon Brother's accidental sale of a few million dollars of stocks:

The error crept in when a clerk at the firm, in translating the order into a format that would be understood by Salomon's computer system, mistakenly put the column showing the total value of the orders into the column showing the number of shares to be traded.

# ✓ U.S. Department of Justice Rulings about Keystroke Capturing

Sanford Sherizen <0003965782@mcimail.com> Fri, 27 Mar 92 19:55 GMT

I have had two separate reports from people working for U.S. Government agencies that the Department of Justice has advised them that trapping of keystrokes is a violation of the Electronic Communications Privacy Act and similar privacy-related legislation. Those who mentioned it to me seemed to imply that the keystrokes being discussed were related to access control/audit measures rather than worker monitoring technology.

Can anyone clarify and/or verify this information? I would be interested in finding out if this interpretation only applies to the Federal Government or to private sector organizations as well? If my information is correct, this may mean that important information security efforts could be considered as illegal activities. The crunch between old laws and new technology grows daily.

Sanford Sherizen, Data Security Systems, Natick, MASS.

# ✓ Test data used for actual operation - once again

Bertrand Meyer @ SOL <bertrand@eiffel.com> Fri, 27 Mar 92 21:09:31 +0100

The following is from Le Canard Enchaine, 25 March 1992. Le Canard Enchaine, a pillar of the French press for 75 years or so, is a satirical and investigative paper, with no known equivalent anywhere else.

The translation, or more correctly the feeble attempt at literal adaptation since the Canard style is basically untranslatable, is by Bertrand Meyer, from whom also the comments in square brackets, some of which refer to notes at the end.

MAD COMPUTER CONS SUPERMARKET CUSTOMERS

TAPPING A THOUSAND BANK ACCOUNTS

Seeing one's bank account being repeatedly debited over a period of several

months, to the credit of a store where you have never set foot - such was the lot of about one thousand customers of a Paris supermarket. Whenever they paid for their expenses using their Visa international card, they were in fact feeding - without their knowledge ... - the coffers of a clothing store, which hadn't asked for it. Overall, because of a computer error, more than 450,000 Francs (US\$ 90,000) was drawn from these involuntary customers.

On October 14, 1991, the manager of the "Codec" [a food supermarket] on the rue des Amandiers [in Paris] notes that his cash registers, driven by a specialized computer program, systematically rejects all payments made by Visa International cards. He calls the PSI Alcatel ISR company, which installed the system and is responsible for its maintenance. In order to find out the source of the problem, a technician [from PSI Alcatel] makes a copy of the store's customer file into one of his company's programs [sic]. Having apparently corrected the error, he sends the file back to Codec.

#### DEBITS UNLIMITED

A few weeks later, a riot or something very close to that erupts at Codec. Dozens of irate customers storm the store's offices: their banking accounts, which were debited normally the previous month [see note 1] after they made some purchases at Codec, are being debited again; but this time it's to the credit of "Gify Center" a clothing store in Nantes [a city in Vendee, on the Atlantic Ocean, several hundred miles from Paris]. Grand total of these double payments: 229,000 F (\$40,000).

In early January 1992, the manager alerts PSI Alcatel. Answer, given without any trace of emotion: PSI Alcatel has know about these computer blunders for several weeks. This is because Gify Center, wondering about this unexpected manna raining full-baked from the computer, had taken the trouble to inform [PSI Alcatel]. As to the poor manager of Codec, being unable to provide any explanation, he is being called a crook by some of his customers.

PSI Alcatel claims to be working hard on the problem - but to no avail since trouble starts again in February. This time it's a store in Vannes [in Brittany, also on the West Coast], also part of the Gify Center chain, which is the beneficiary. Five hudred clients are affected; some of them, according to the Codec manager, are even debited four times for the same amount. [??]

At this stage the police, being flooded with complaints, opens an investigation and summons the poor Codec manager. Not hard to understand why: many of the affected customers have had to pay interest penalties to their banks [see note 2], since their accounts have had overdrafts because of these repeated payments. Others have had to pay penalties for returned checks, or have been on the brink of having their bank cards cancelled.

#### COMPUTER HICCUPS

By dint of hard work, PSI Alcatel at last discovers the source of all these computer follies. [Perhaps someone should suggest a subscription to RISKS?] The technician, who had copied the Codec's customer file into his own program [sic and resic, to use a favorite Canard expression] for the purpose of debugging it, had forgotten to erase the file. A fateful mistake: every time PSI Alcatel sold their program for managing cash registers, they were also unwittingly selling the Codec's customer file. After that, whenever the program had been inserted into a store's computer, it would direct the banks to debit the accounts of the customers recorded in that file.

One piece of good news: PSI Alcatel claims to have sold this over-filled program to no one else than Gify Center. The customers of the rue des Amandiers Codec have avoided the worst: since Gify Center owns about forty stores in France, that's the number of times the mad computers could have emptied their accounts.

[End of article]

[Notes for foreign readers:

[1] The most common use of credit cards in France is as ``debit cards''; i.e. they are tied to a bank account and expenses are automatically debited at the end of the month.

[2] Overdraft is less of an abnormal situation in France than in e.g. the US. Most banks will tolerate some overdraft as long as the situation doesn't get too serious. It's actually a fairly juicy situation for them since they charge rather high ``agios'' (translated above by ``interest penalties''.)]

[General note: I am surprised by the relatively small amounts of money involved.]

# 🗡 Re: UA 747 Lost Door

Brian Boutel <brian@comp.vuw.ac.nz> Tue, 24 Mar 1992 16:14:22 +1200

It's worth noting that the revision in the official story, that an electrical, not mechanical fault was responsible, is entirely due to the persistance of one man, the father of one of the passengers lost in the accident. He formulated this theory, and persued it with United and Boeing, even, I believe, got permission to be present when the door was recovered from the bottom of the Pacific. The new finding vindicates his stand, and without his efforts, it is unlikely that the truth would have been found.

--brian

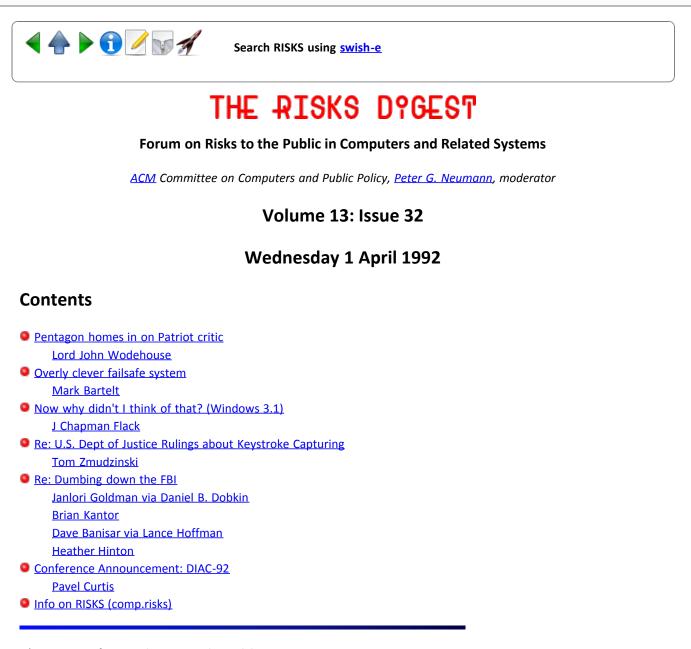
Brian Boutel, Computer Science Dept, Victoria University of Wellington, PO Box 600, Wellington, New Zealand Phone: +64 4 471-5328 Fax: +64 4 495-5232



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 13: Issue 31



# Pentagon homes in on Patriot critic

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 30 Mar 92 11:36:00 GMT

>From the New Scientist 28 March 1992 - a follow up to "Patriot missiles misled by `accidental' decoys" (<u>RISKS-13.19</u>).

The Pentagon is accusing one of its scientific critics of publishing secret data on the Patriot missile. The scientist, Ted Postol of MIT, says that all his information came from published sources and his own calculations.

The row began after Postol published a 50-page article on the Patriot's performance in the Gulf War in the journal "International Security". The article presents evidence that the Patriot missed most, and perhaps all, the Iraqi warheads it was fired at. (New Scientist 15 Feb 1992)

Postol has worked for the US Navy and consulted nuclear weapon laboratories in the past. He has a security clearance that allows him access to classified information. But he says he purposely stayed away form all classified briefings on the Patriot so that he could make his conclusions public.

On 13 March, Postol was visited by an investigator from the Defense Investigative Service. The DIS officer wanted Postol to attend a classified meeting to discuss where he had obtained the information for his article. Postol refused, saying that if he did, he would really learn secret information about the Patriot, which would prevent him from talking about it.

The investigator then informed Postol that he would have to stop discussing the article in public anyway, because the US Army had decided that it contained secret data. If Postol refused, he would be in violation of his secrecy agreement with the government and could lose his security clearance.

Postol says he found his order incredible, and asked to have it in writing. More than a week later, on 19 March, he was told that a letter was waiting for him at the Mitre Corporation, a nearby military contractor. In a Kafkaesque twist. the letter itself was classified, so Postol is refusing to read it.

Last week, the Pentagon disclosed that the Raytheon Corporation, which manufacturers the Patriot, had started the entire affair. Raytheon executives had sent a copy of Postol's article to the Army. suggesting that it might contain secret information.

Pete Williams, the Pentagon spokesman, tried to play down the affair last week. He told reporters that the DIS was carrying out a routine investigation and "no final determination has been made" on whether Postol's article contained secrets.

A Congressional committee has taken up Postol's cause, and is investigating whether the Pentagon is abusing its classification system to silence a critic.

[I feel that Postol must have a point, given the rather backdoor methods being used to stop him blowing the whistle any more.]

Lord John - the programming peer

## verly clever failsafe system

Mark Bartelt <sysmark@orca.cita.utoronto.ca> Mon, 30 Mar 92 13:27:00 EST

The following appeared in my mailbox. (Don't know the name of the person who originally sent it; I was at the end of a moderate-sized forwarding chain.)

On Peter Ross's ABC-TV arts show on Sunday Afternoon, the avant garde composer John Cage was featured performing his 4'33". It consists of the performer(s), armed with a stopwatch, sitting silently on stage for four minutes 33 seconds, with the music consisting of whatever noises come from the audience or outside the auditorium. The TV performance went well, but the ABC was caught out by technology - a fail-safe device turns off studio transmission if there's more than 90 seconds of silence, and puts up a test pattern. It went into operation three times during the performance.

Mark Bartelt, Canadian Institute for Theoretical Astrophysics 416/978-5619

## Now why didn't I think of that? (Windows 3.1)

j chapman flack <chap@art-sy.detroit.mi.us> Sun, 22 Mar 92 18:13:46 GMT

Just read in a direct-mail promotional piece for Microsoft Windows 3.1:

You may be wondering \_how\_ Windows version 3.1 reduces application errors and system crashes. One of the most powerful additions to Windows 3.1 is "parameter validation." Parameter validation means that when information is passed from an application to the Windows operating system, Windows checks the information to make sure it is valid.

"Focus on Windows," page 8. Chap Flack chap@art-sy.detroit.mi.us

## Ke: U.S. Dept of Justice Rulings about Keystroke Capturing

"zmudzinski, thomas" <ZMUDZINSKIT@imo-uvax6.dca.mil> 30 Mar 92 10:45:00 EST

DEFENSE INFORMATION SYSTEMS AGENCY Dept: DNSO/DISM Tel No: 703 285 5459 (DSN) 356

In <u>RISKS-13.31</u>, Sanford Sherizen wrote:

<> I have had two separate reports from people working for U.S. Government agencies that the Department of Justice has advised them that trapping of keystrokes is a violation of the Electronic Communications Privacy Act and similar privacy-related legislation. Those who mentioned it to me seemed to imply that the keystrokes being discussed were related to access control/audit measures rather than worker monitoring technology.

Unfortunately, correct. The situation is roughly analogous to having to post signs saying that there are TV cameras monitoring your condo.

<> Can anyone clarify and/or verify this information? I would be interested in finding out if this interpretation only applies to the Federal Government or to private sector organizations as well? I don't know about the Electronic Communications Privacy Act, but National Telecommunications and Information Systems Security Directive (NTISSD) NO. 600, "Communications Security (COMSEC) Monitoring," 10 Apr 90 (FOUO), makes it a requirement that users of Government telecommunications systems be notified in advance that their use of these systems constitutes consent to monitoring for COMSEC purposes. (No, I don't have a copy.)

I'm not a lawyer (my parents are married), but I've been given to understand that "Government telecommunications systems" means ANY computer or network whether OWNED or merely FUNDED by the Government. (Can you say "nearly every system in the U.S."? I knew you could!) If you have any question as to the applicability to your own situation, I suggest you hire a member of the Legal Guild who can spell "telecommunications".

F.Y.I., DISA (via DDN Security Bulletin 9123)\* strongly "recommended" that all DDN hosts insert one or the other of the following in their "WELCOME" messages, either:

"GOVERNMENT TELECOMMUNICATIONS SYSTEMS AND AUTOMATED INFORMATION SYSTEMS ARE SUBJECT TO A PERIODIC SECURITY TESTING AND MONITORING TO ENSURE PROPER COMMUNICATIONS SECURITY (COMSEC) PROCEDURES ARE BEING OBSERVED. USE OF THESE SYSTEMS CONSTITUTES CONSENT TO SECURITY TESTING AND COMSEC MONITORING."

-- or, for those sites with limited bandwidth, --

"USE CONSTITUTES CONSENT TO SECURITY TESTING AND MONITORING."

It's my understanding that the wording of these "un-WELCOME" messages was worked out with no little blood on the rug.

<> If my information is correct, this may mean that important information security efforts could be considered as illegal activities.

Very true. For example, an "alleged penetrator" (prosecuting attorneys prefer to avoid the H(acker) word as "too warm and fuzzy") was monitored while committing (what I'd consider to be) electronic breaking and entry. He got off because he hadn't been warned that he was being monitored. (This may be hearsay, but it is NOT apocryphal; I know some of the parties involved and have suppressed the names to protect those found Not Guilty.)

<> The crunch between old laws and new technology grows daily.

This is news? (Rhetorical question)

Tom Zmudzinski, Non-Specializing Specialist in AIS Security for the Defense Information Systems Agency

\* DDN Security Bulletin 9123, 5 November 1991, may be obtained via FTP (or Kermit) from NIC.DDN.MIL [192.112.36.5] using login="anonymous" and password="guest". The bulletin pathname is SCC:DDN-SECURITY-9123.

# ✓ Dumbing down the FBI

"Daniel B. Dobkin" <dbd@ans.net> Mon, 30 Mar 92 20:40:26 EST

Lance Hoffman's posting on Friday mentioned the New York Times Op-Ed dialogue between FBI Director William Sessions and Janlori Goldman, director of the ACLU Privacy and Technology Project. Kurt Sauer posted Director Session's article; at the risk of preaching to the choir, herewith is Ms. Goldman's reply.

Keeping an Ear on Crime: Why Cater To Luddites?

#### By Janlori Goldman

The Federal Bureau of Investigation says advances in the telecommunications industry are likely to make it difficult to use its old-fashioned wiretapping techniques to listen in on telephone conversations. The F.B.I.'s solution, in legislation the Justice Department is asking Congress to pass, is to force the telecommunications and computer industries to redesign their modernized systems to accommodate the bureau's needs. Unfairly, the F.B.I. wants consumers to pay for it through rate increases and higher equipment costs. The telecommunications and computer industries both oppose a bill that would mandate such sweeping regulations.

The proposal makes the bureau look like Luddites, the 19th century English weavers who smashed new machines that they claimed put them out of work. Instead of keeping up with new developments, the F.B.I. wants to freeze progress.

It is wrongheaded and dangerous to require the industry to put surveillance first by slowing innovation and retarding efficiency. How can the F.B.I. justify this policy at home while the White House is wringing its hands over U.S. competitiveness in the international market?

The F.B.I. fears that new digital technology will make it difficult, even impossible, to listen in on conversations by using traditional wiretapping equipment. The new technology converts voices and data into electronic blips and reconverts the blips into voices and data near the receiving end on high-speed fiberoptic lines.

The bureau overstates its concern. The telecommunications industry says it is not aware of a single instance in which the F.B.I. has been unable to tap a line because of the widespread new technology. Even the Director, William S. Sessions, admitted in a Congressional hearing last week that no warrant has been issued that could not be executed.

At issue is the F.B.I.'s ability to wiretap in the future. But the answer is not a legislative fix that freezes technology. The F.B.I. is not only asking the industry to dumb down existing software, it wants to prohibit it from developing new technologies that might interfere with the Government's ability to intercept various oral and electronic communications. The proposed restrictions not only cover phone companies but also on-line computer services (such as as Prodigy and Compuserve), electronic mail systems and bulletin boards, and switchboards.

The F.B.I. says its proposal only seeks to preserve its legal authority to wiretap. Actually, it wants to expand the power of the Federal Communications Commission, which regulates the telecommunications industry, to make the F.B.I.'s needs a priority in designing new technologies. In its legislation, the Government threatens to impose a \$10,000-a-day fine on companies that develop technologies that exceed the F.B.I.'s technical competence. The F.B.I. has it backward. If the Government wants to engage in surveillance, it must bear the burden of keeping pace with new developments. Last year, Congress appropriated \$80 million for a five-year F.B.I. research effort focused on telecommunications advances.

There is a serious risk that rollbacks in advances may make telecommunications networks more vulnerable to unauthorized intrusion. One of the industry's main goals is to design secure systems that thwart illegal interception of electronic funds transfers, proprietary information and other sensitive data.

The F.B.I. is not the only agency trying to block progress. The National Security Agency has tried to put a cap on the private development of technology in encryption, the electronic encoding of data to guard against unauthorized use.

As the private sector develops more effective encryption codes to protect information in its data bases, the N.S.A. worries that it may have trouble breaking such codes in its intelligence gathering overseas. The agency is denying export licenses for certain encryption codes, thus inhibiting the private sector's development and use of the technology. Congress should defeat the proposal. Otherwise, we may be prohibited from erecting sturdy buildings if the thick walls prevent an F.B.I. agent from eavesdropping on a conversation through a cup pressed to a wall.

### Ke: dumbing down new systems (FBI vs digital phones)

Brian Kantor <brian@UCSD.EDU> Fri, 27 Mar 92 21:00:18 -0800

Every telephone switch I have ever encountered had the capability of monitoring individual conversations, even when those conversations are multiplexed together with other connections in the switch. While my experience is not as wide as others in the telephone field, it would seem to me that such a monitoring capability is an essential switch design element for diagnostic purposes, if nothing else.

Thus I do not believe that the FBI has any need for this law; they need only take their court order to the telephone company and they will be provided with the tap they have been authorized.

No, it seems to me that the ONLY purpose the FBI has in proposing such a law would be so that it can make telephone taps WITHOUT the cooperation of the telephone company. Presumably, the only reason for not wanting the cooperation

of the telephone company is that the FBI in such cases might well not have the cooperation of the court either - in other words, what they are asking for is the ability to make warrantless taps.

End-to-end encryption, of course, would NOT fit this model. Nor would it be prevented by this law, since encryptors can be fitted to any phone without the cooperation of the phone company.

- Brian

### Washington Post editorial on dumbing down new systems (fwd)

Dave Banisar, CPSR Washington <banisar@washofc.cpsr.org> Fri, 27 Mar 1992 14:15:25 EDT

[Forwarded to RISKS by Lance J. Hoffman <hoffman@seas.gwu.edu>

The Washington Post March 26, 1992 Back to Smoke Signals?

The Justice Department spent years in court breaking up the nation's telecommunications monopoly in order to foster competition and technological advances. Now the same department has gone to Congress asking that improvements in telecommunications technology be halted, and in some cases even reversed, in the name of law enforcement. The problems facing the FBI are real, but the proposed solution is extreme and unacceptable on a number of grounds.

Wiretaps are an important tool in fighting crime, especially the kind of large-scale, complicated crime -- such as drug conspiracies, terrorism and racketeering -- that is the responsibility of the FBI. When they are installed pursuant to court order, taps are perfectly legal and usually most productive. But advances in phone technology have been so rapid that the government can't keep up. Agents can no longer just put a tap on phone company equipment a few blocks from the target and expect to monitor calls. Communications occur now through regular and cellular phones via satellite and microwave, on fax machines and computers. Information is transmitted in the form of computer digits and pulses of light through strands of glass, and none of this is easily intercepted or understood.

The Justice Department wants to deal with these complications by forbidding them. The department's proposal is to require the Federal Communications Commission to establish such standards for the industry "as may be necessary to maintain the ability of the government to lawfully intercept communications." Any technology now in use would have to be modified within 180 days, with the costs passed on to the rate payers. Any new technology must meet the suitable-for- wiretap standard, and violators could be punished by fines of \$ 10,000 a day. As a final insult, commission proceedings concerning these regulations could be ordered closed by the attorney general.

The civil liberties problems here are obvious, for the purposeful designing of telecommunications systems that can be intercepted will certainly lead to invasions of privacy by all sorts of individuals and organizations operating without court authorization. Further, it is an assault on progress, on scientific endeavor and on the competitive position of American industry. It's comparable to requiring Detroit to produce only automobiles that can be overtaken by faster police cars. And it smacks of repressive government.

The proposal has been drafted as an amendment rather than a separate bill, and there is some concern that it will be slipped into a bill that has already passed one house and be sent quietly to conference. That would be unconscionable. We believe, as the industry suggests, that the kind of informal cooperation between law enforcement agencies and telecommunications companies that has always characterized efforts in the past, is preferable to this stifling legislation. But certainly no proposal should be considered by Congress without open and extensive hearings and considerable debate.

### Re: The FBI Needs Industry's Help--OpEd in NYT

Heather Hinton <heather@hub.toronto.edu> Mon, 30 Mar 1992 10:22:20 -0500

>... When I read between the lines, it

>sounds as if Mr. Sessions doesn't want us to use data security which employs >end-to-end encryption; perhaps other RISKS-DIGEST readers will draw different >conclusions.

I agree with your conclusions. What I want to know, is wire-tapping really the best way of catching criminals? Sounds like this fellow is belly-aching because his comfy method of listening to other peoples private lives may be in jeopardy!

Just wait till the FBI demands that all encryption keys and routines be registered with the FBI for 'security' reasons!

Heather M Hinton (mail: heather @ hub.toronto.edu) Dept of Electrical Engineering, 10 King's College Road, University of Toronto

### ✓ Conference Announcement: DIAC-92

Pavel Curtis <Pavel@parc.xerox.com> Sat, 21 Mar 1992 21:26:11 PST

Are computers part of the problem or ... ?

DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING DIAC-92 Symposium Berkeley, California U.S.A Sponsored by Computer Professionals for Social Responsibility May 2 - 3, 1992 8:30 AM - 5:30 PM

The DIAC Symposia are biannual explorations of the social implications of computing. In previous symposia such topics as virtual reality, high tech weaponry, computers and education, affectionate technology, computing and the disabled, and many others have been highlighted. Our fourth DIAC Symposium, DIAC-92, offers insights on computer networks, computers in the workplace, national R&D priorities and many other topics.

DIAC-92 will be an invigorating experience for anyone with an interest in computers and society.

May 2, 1992

Morris E. Cox Auditorium 100 Genetics and Plant Biology Building (NW Corner of Campus) University of California at Berkeley

8:30 - 9:00 Registration and Continental Breakfast9:00 - 9:15 Welcome to DIAC-92, Doug Schuler, DIAC-92 Chair9:15 - 10:15 Opening Address

Building Communities with Online Tools - John Coate, Director of Interactive Services, 101 OnLine

When people log into online communication systems, they use new tools to engage in an ancient activity - talking to each other. Systems become a kind of virtual village. At the personal level they help people find their kindred spirits. At the social level, they serve as an important conduit of information, and become an essential element in a democratic society.

John was known as a Community Builder at the WELL (Whole Earth 'Lectronic Link) where he worked tirelessly to build the WELL into a place with clearly recognizable social cohesion.

10:15 - 10:45 Break 10:45 - 11:15 Presentation

Computer Networks in the Workplace: Factors Affecting the Use of Electronic Communications - Linda Parry and Robert Wharton, University of Minnesota

11:15 - 11:45 Presentation

Computer Workstations: The Occupational Hazard of the 21st Century - Hal Sackman, California State University at Los Angeles

11:45 - 12:15 Presentation

MUDDING: Social Phenomena in Text-Based Virtual Realities - Pavel Curtis, Xerox PARC

12:15 - 1:30 Lunch in Berkeley 1:30 - 2:00 Presentation

Community Memory: a Case Study in Community Communication - Carl Farrington and Evelyn Pine, Community Memory 2:00 - 3:15 Panel Discussion

Funding Computer Science R&D

What is the current state of computer science funding in the U.S.? What policy issues relate to funding? Should there be a civilian DARPA? How does funding policy affect the universities? industry? Organized by Barbara Simons, IBM Almaden Research Center. Moderated by Mike Ubell, Digital Equipment Corporation.

Panelists include

Mike Harrison, Computer Science Division, U.C. Berkeley Gary Chapman, 21st Century Project Director, CPSR, Cambridge Office Joel Yudken, Project on Regional and Industrial Economics, Rutgers University

3:15 - 3:45 Break 3:45 - 5:00 Panel Discussion

Virtual Society and Virtual Community

This panel looks at the phenomenon of virtual sociality. What are the implications for society at large, and for network and interactive system design in general? Moderated by Michael Travers, MIT Media Lab.

Panelists include:

Pavel Curtis, Xerox PARC Allucquere Rosanne Stone, University of California at San Diego

5:00 - 5:15 Closing Remarks, Eric Roberts, CPSR President

May 3, 1992 Tolman Hall and Genetics and Plant Biology Building (NW Corner of Campus) University of California at Berkeley

8:30 - 9:00 Registration and Continental Breakfast

Workshops in Tolman Hall

The second day will consist of a wide variety of interactive workshops. Many of the workshops will be working sessions.

9:00 - 10:40 Parallel Workshops I

Toward a Truly Global Network - Larry Press, California State University, Dominguez Hills

Integration of an Ethics MetaFramework into the New CS Curriculum - Dianne Martin, George Washington University

A Computer & Information Technologies Platform

- The Peace and Justice Working Group, CPSR/Berkeley

Hacking in the 90's: Toward a Hacker's League - Steve Sawyer, CJS Systems - Lee Felsenstein, Golemics, Incorporated, Berkeley CA 10:40 - 11:00 Break 11:00 - 12:40 Parallel Workshops II Designing Computer Systems for Human (and Humane) Use - Batya Friedman, Colby College Examining Different Approaches to Community Access to Telecommunications Systems - Evelyn Pine Third World Computing: Appropriate Technology for the Developed World? - Philip Machanick, University of the Witwatersrand, South Africa Can We Talk? Engineers, Machinists, and the Barriers to a Skill-Based Approach to Production - Sarah Kuhn, University of Massachusetts -- Lowell 12:40 - 1:40 Lunch in Berkeley 1:40 - 3:20 Parallel Workshops III Defining the Community Computing Movement: Some projects in and around Boston - Peter Miller, Somerville Community Computing Center Future Directions in Developing Social Virtual Realities - Pavel Curtis, Xerox PARC Work Power, and Computers - Viborg Andersen, University of California at Irvine Designing Local Civic Networks: Principles and Policies - Richard Civille, CPSR, Washington Office 3:20 - 3:40 Break 3:40 - 5:00 Plenary Panel Discussion Work in the Computer Industry --- This panel discussion is free to the public. --Morris E. Cox Auditorium 100 Genetics and Plant Biology Building (NW Corner of UCB Campus) Is work in the computer industry different from work in other

industries? What is the nature of the work we do? In what ways is our situation similar to other workers in relation to job security, layoffs, and unions? Moderated by Denise Caruso, editor of Digital Media.

Panelists include

Dennis Hayes, writer and author of "Behind the Silicon Curtain" John Markoff, New York Times (tentative)

5:00 - 5:15 Closing remarks, Coralee Whitcomb, CPSR Board

There will also be demonstrations of a variety of community networking and MUDDING systems during the symposium.

Sponsored by Computer Professionals for Social Responsibility P.O. Box 717 Palo Alto, CA 94301

DIAC-92 is co-sponsored by the American Association for Artificial Intelligence, the IEEE Society for Social Implications of Technology, and the Boston Computer Society Social Impact Group, in cooperation with ACM SIGCHI and ACM SIGCAS. DIAC-92 is partially supported by the National Science Foundation under Grant No. DIR-9112572, Ethics and Values Studies Office.

CPSR is a non-profit, national organization of computer professionals concerned about the social implications of computing technologies in the modern world. Since its founding in 1983, CPSR has achieved a strong international reputation. CPSR has over 2500 members nationwide with chapters in over 20 cities.

If you need additional information please contact Doug Schuler, 206-865-3832 (work) or 206-632-1659 (home), or Internet dschuler@cs.washington.edu.

--- DIAC-92 Registration ---

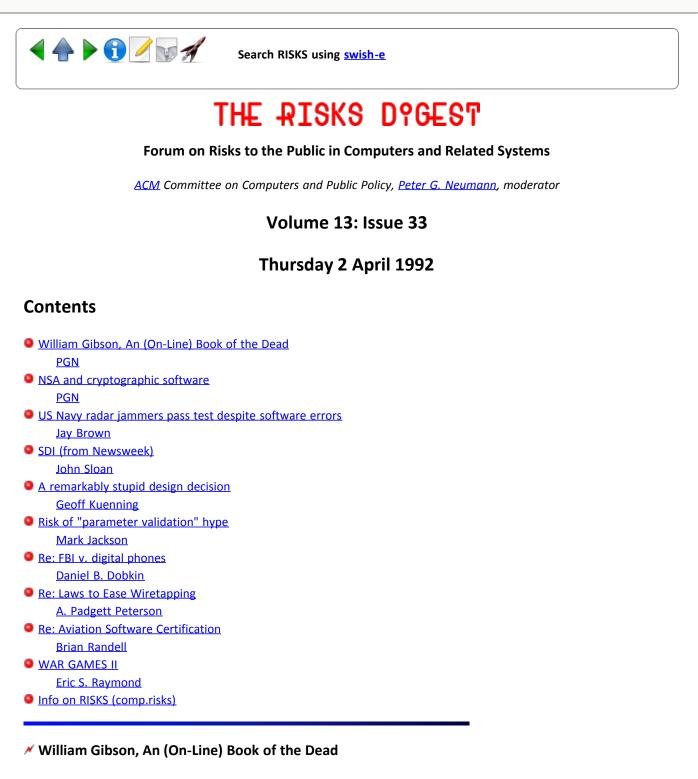
Registration includes proceedings, continental breakfasts, and refreshments during breaks. Proceedings and are also available by mail.

Send completed form with check or money order to:

DIAC-92 Registration
P.O. Box 2648
Sausalito, CA, 94966
USA
Name
Address:
City:
City:
Electronic mail:
Symposium registration:

CPSR Member (or AAAI, BCS, IEEE SSIT, ACM SIGCAS, ACM SIGCHI) \$40 \_\_\_\_

	\$50				
Student	\$25				
Proceedings Only	\$20 _	_			
Proceedings Only	(foreign)	\$25			
New CPSR Membe	ership (includes DIAC-	92 Registration)	\$80		
One day registration					
	AAAI, BCS, IEEE SSIT,				
Non-member	\$30		, denný († 25 <u>–</u>		
Student	\$15				
Student	, <u>, , , , , , , , , , , , , , , , , , </u>				
Additional Donation	on \$				
Total enclosed		\$			
-=-=-=-=-=	- = - = - = - = - = - = - =	- = - = - = - = - =			
There are TWO build	dings called Genetics a	nd Plant Biology at	UCB. We		
are using the smalle	r, southern one of the	two. There are UC	parking		
lots near the NW sid	le of the campus for \$	3.00 a day. Parking	meters use		
quarters (\$.25).					
,					
,					
,					
				_	
<	🖌 👽 🚀 — Se	arch RISKS using <u>sw</u>	vish-e		
	🖉 👽 🚀 — Se	arch RISKS using <u>sw</u>	<u>vish-e</u>		
	Se	arch RISKS using <u>sw</u>	<u>vish-e</u>		
◀ ♠ ▶ ĵ	th the web pages to th		vish-e		



"Peter G. Neumann" <neumann@csl.sri.com> Thu, 2 Apr 92 9:08:13 PST

William Gibson, well known for his "Neuromancer" (which in 1986 anticipated what is today known as virtual reality), has a new book, "Agrippa (A Book of the Dead)" that apparently will be available ONLY in computer-diskette form, according to Entertainment Weekly.

As reported in the San Francisco Chronicle (31 Mar 1992, p.D3), "Gibson plans to infect the disk with a virus that will make it impossible to transfer the

#### text to paper."

This supposed "virus" (more like a logic bomb or a confinement lock?) will undoubtably present an interesting challenge to MSDOS crackers, antiviralists, virtual realists, and foreign ripoffs. If it were to run on Unix, where you can external to the program trivially pipe the output to a file, at least the text would be easy to capture. However, perhaps this is really a situation in which it is the graphical screen image that is relevant rather than the words. Digitized sound would also make it hard to transfer to paper.

There is also the likelihood that a succession of home-grown purgated editions might appear, with incremental changes in the dialogue, visuals, and plot line. You don't like the ending? You want pornographic augmentations? Roll your own modifications! Tinkering is generally easier than creating in the first place. So, the book also needs some sort of integrity lock (checksum or crypto seal [is a sea-lion a cryptoseal?]) to provide tamper detection; however, many such schemes can be defeated by careful modifications that continue to satisfy the check. But, if Gibson has come up with an interactive, interpretively developed book that creates its own virtual reality on the screen, that could be quite an exciting development.

[Note: It is important not to confuse the SF Chronicle noted above with the other publication with the same handle, the Science Fiction Chronicle, although sometimes it is hard to tell the difference.]

### NSA and cryptographic software

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 2 Apr 92 9:23:37 PST

The NSA and the Software Publishers' Association appear to have reached an agreement that would allow some exports of cryptographic software, as long as the keys are constrained to be sufficiently short. The net effect is a slight but potentially useful improvement over what was previously exportable. [Source: An article, NSA May Loosen Curbs on Software Sales Abroad, by Don Clark, Chronicle Staff Writer, San Francisco Chronicle, 24 Mar 1992, p.C1]

Now that NSA and RSA have come a little closer, we need to bring in BSA (the Boy Scouts of America). Be prepared! Imagine, a merit badge for cryptography?

[For some background on RSA, see Burt Kaliski's contribution on the free (to noncommercial users) RSAREF privacy-enhanced mail toolkit, <u>RISKS-13.22</u>.]

### ✓ US Navy radar jammers pass test despite software errors

Jay Brown <jbrown@phoebus.ncsc.navy.mil> Thu, 2 Apr 92 08:02:29 CST

There was a report last week on CNN Headline News about the US Navy improperly certifying radar jamming equipment for Navy jets (I think the F-14 and the F/A-18 were mentioned). According to the report, the Navy tested and certified

these jammers despite the fact that the equipment failed several tests or did not meet all the criteria for certification. As a consequence, some congressional subcommittee or another was investigating the Navy's certification procedures. The Navy's excuse for certifying these systems despite the failed tests was to blame the failures on software errors, according to the report.

The report did not mention who manufactured the radar jammers or who wrote the software in question.

-- John L. Brown, jbrown@phoebus.ncsc.navy.mil

### Newsweek, March 23,1992, on SDI

John Sloan <jsloan@niwot.scd.ucar.EDU> Sat, 28 Mar 92 12:16:32 MST

The March 23, 1992 edition of \_Newsweek\_ features an article critical of research related to the Strategic Defense Initiative. The article is titled "Safety Net Full of Holes" (pp. 56-59), written by Sharon Begley and Daniel Glick. It contains this reassuring passage:

"[The] Pentagon disagrees that deploying a spaceand ground-based defense system poses significant technical challenges. The complexity of the software required to coordinate Star Wars, for instance, is no more daunting than programs that control nuclear reactors, it says."

Now we can all breath a sigh of relief. [ All typos are mine. ]

John Sloan, NCAR/SCD, jsloan@ncar.ucar.edu

### A remarkably stupid design decision

Geoff Kuenning <desint!geoff@uunet.UU.NET> Thu, 2 Apr 92 03:03:19 PST

I just had to pass this one on because it was so funny/sad. A client told me today of a consultant who designed a menu-driven system to be used by accountants for financial purposes. Needing a special character to signify "return to main menu", he chose one that "nobody uses" (his words). The character? The dollar sign!

Needless to say, on the first day the software was installed, my client got a frantic call. "Every time I try to enter a dollar amount, it pops me back to the menu!"

Sigh. Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

## Kisk of "parameter validation" hype

Mark Jackson <MJackson.wbst147@xerox.com> Thu, 2 Apr 1992 06:15:04 PST

So Microsoft is touting "parameter validation" as a bold new innovation. You forgot to cite the obvious Risk: someone's inevitable attempt to \*patent\* parameter validation. . .

### Ke: FBI v. digital phones (Kantor, <u>RISKS 13.32</u>)

"Daniel B. Dobkin" <dbd@ans.net> Thu, 2 Apr 92 10:13:21 EST

Brian Kantor notes that a monitoring capability is an essential diagnostic element of any telephone switch, digital or analog. He suggests that the only purpose conceivable for a law such as the FBI proposes is to enable wiretaps without Telco cooperation; this in turn is most likely to occur when the FBI doesn't have a proper warrant, either. Hence, "[W]hat they are asking for is the ability to make warrantless taps."

In fairness to the FBI, there are other possibilities, such as when a Telco employee is himself the subject of an investigation. Not much, I agree, but let's try to assume that the Bureau's motivation is pure, even if its proposed implementation isn't.

#### Laws to Ease Wiretapping

## A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Wed, 1 Apr 92 22:37:48 -0500

This makes the second time in recent months we have heard of government initiatives to make wiretapping of data traffic easier. Interestinly, there are a couple of companies currently working on devices (and must admit I have been prodding them for a couple of years) that should make it an order of magnitude more difficult:

For some time now, I have been concerned about tapping, particularly when performing my daily security duties while at conferences. Currently I rely on a "smart card" or dynamic access device for one-time passwords to avoid spoofing. About two years ago the following thought crossed my mind:

Years ago when maintaining KY-26 cryptographic equipment, (my AFSC was 306mop0) brave souls used to bring up encrypted channels "blind" to minimise time away from the poker game. Instead of changing the transmit side first and using the receive side to verify reception, we used to change both sides at once by taking a pre-established count to go "bravo india" and create a synchronized duplex connection. If we could communicate, we would know that it had worked (what was done if it did not is not disclosable but involved the butt end of a large

#### screwdriver).

Similarly, a couple of years ago I was talking to one of the major vendors of "dynamic access control devices" about use to provide full encryption of all traffic. Currently, the way such a system works is that when a login occurs, the host sends out a multi-digit "challenge". In my case, I enter the challenge followed by a PIN into a card which then calculates a reply. I send back the reply as a password that lets me into the system.

What I postulated was that instead of sending the reply back to the host, it be fed into my laptop as the seed for encryption. The laptop then sends a "bravo india" to the host telling it to start encryption. Since the host knows what the reply should be, it uses that as its own seed. If both sides are then able to communicate, they authenticate each other simultaneously while providing full encryption of all following traffic.

One of the major problems was loss of synch from line noise, but the current crop of error-correcting modems has made such encryption not only feasible but also easy and at whatever level (DES, RSA, ...) is desired.

## Ke: Aviation Software Certification

<Brian.Randell@newcastle.ac.uk> Mon, 30 Mar 92 12:56:51 BST

Last month I sent to RISKs a copy of an article that appeared in the (UK) Computer Weekly on 6 February which carried the headline "Experts warned CAA before Airbus disaster". Attached is a letter, from the experts concerned, complaining at this article. This letter was I understand published by Computer Weekly on February 13, and has just been drawn to my attention. Despite the delay, I suggest that it be included in RISKs, in view of the comments it makes on the original article.

Brian Randell

AIRBUS SOFTWARE IN THE CLEAR

\_\_\_\_\_

We are the three BCS "software experts" who visited the CAA in January to discuss the new draft standard for software in aircraft systems D0-178B.

We believe that it is misleading that you linked our technical visit to the CAA to the subsequent A320 Airbus crash. There is no evidence of any fault in any safety-critical software on the A320 Airbus crash. It is too early to know the causes of the crash and irresponsible to imply that we were in any way trying to "warn the CAA" about the A320.

Our concerns about the draft D0-178B are technical and relate to its inadequacy as a basis for objective certification of the reliability of software in airborne systems. All modern passenger aircraft contain safety-critical software and our comments to the CAA did not relate to any specific aircraft. The CAA received our comments constructively and readily agreed to pass each criticism to the international team which is reviewing the draft standard.

Bev Littlewood, Martyn Thomas, Brian Wichmannn

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

### 🗡 WAR GAMES II

Eric S. Raymond <eric@snark.thyrsus.com> 2 Apr 92 02:34:52 GMT

WAR GAMES II or How I Learned To Start Worrying and Hate The Bomb

[posted to comp.risks; an incomplete version previously went to other groups]

Some of my friends call me an `improbability vortex' --- the kind of person weird stuff just naturally happens around. Occasionally I manage to to forget why; my life doesn't seem bizarre to \*me\*. Then, something happens to remind me...

Wednesday, March 25 1992: a fairly ordinary day in the life of Eric Raymond, Boy Hacker. Shower, read netnews, phone calls, some revision on the clone hardware buyer's guide I've been working on for comp.unix.sysv386. Will the top ten vendors go for my idea of a competitive "UNIX Dream Machines Bake-Off"? Hmm...well, Swan Tech wants to sign up, that's a start. Ah, the mail's in.

Riffle, riffle. What's this? Forwarded from MIT Press. Something about the book, no doubt...

The Book: if you don't know it already, I edited a lexicon called \_The\_New\_Hacker's\_Dictionary\_ (MIT Press, 1991, ISBN 0-262-68069-6). It's all about hacker language and folklore. Sold 14,000 copies in its first seven months, got rave reviews everywhere, good stuff like that. Got my first nut-case letter about a month back --- always heard that was supposed to happen to authors. Some of the fallout has been weird. Ouch, fallout --- \*bad\* choice of words. Back to our story.

Hm. From ISPNews. INFOSecurity Product News. Eh? Never heard of them; sounds like some trade rag for professional paranoids. Computer form on the inside; addressed to ERIC RAYMOND EDITOR, THE MIT PRESS, MASS INST OF TECHNOLOGY, CAMBRIDGE MA 02142. I see what happened; the Press's editorial address miscegenated with my book credit in someone's mailing-list software, and some clerical droid at the Press didn't look at content and forwarded a piece of mail that should have stayed in-house.

What we've got here is, oh, yeah, must be a report from the magazine's

bingo card. Reader service; they circle numbers, you get a bunch of product info requests. OK, who wants to know about my book? Maybe I'll give them a surprise and answer it myself. They probably all think the book is a how-to manual for crackers. Damn all journalists for what they did to the word "hacker", anyhow...

There were four. First one:

DAVID CARGILL SYSTEMS A GUARDIAN LIFE INS STE 201 888 SEVENTH AVE NEW YORK NY 10106

Oh, boring, I thought to myself. Actually he turned out not to be; I spoke with him, later, and the guy turns out to be an old UNIX hand who, when I explained what the book is really about, cheerfully expatiated on Cargill's Theory of Fat Electrons.

See, Con Edison sucks its line current out of the big generators with a pair of coil taps located near the top of the dynamo. When the normal tap brushes get dirty, they take 'em off line to clean up, and use special auxilliary taps on the \*bottom\* of the coil. Now (sez Cargill) this is a problem, because when they do that they get not ordinary or `thin' electrons, but the fat'n'sloppy electrons that are heavier and so settle to the bottom of the generator. These flow down ordinary wires OK, but when they have to turn a sharp corner (like in an IC via) they get stuck. This is what causes computer glitches.

I laughed, said "You sound like a man who wants to hear about {quantum bogodynamics}" and directed him to the on-line version of the book at prep. Back to our story...

Next guy...

BRADLEY H EDWARDS SEC SPE SECURITY-SAFETY CONSULTS PO BOX 536 TOPEKA KS 66601

Well, the phone number attached to this one was out of service. Security Specialist, eh? For sure he's got the cracker/hacker bug on the brain. Then my eyeballs tripped over the third address

PAMELA D MILLER CHIEF USSPACE COM STOP 4 J2C/SSO-C CHEYENNE MTN AFB CO 80914

and I went into the mental equivalent of TILT TILT TILT. Now, any of you who ain't congenital idiots raised in a rain barrel somewhere on the butt-end of nowhere will already have decoded that address to "U.S. Space Command, Cheyenne Mountain Air Force Base". Yeah, that's right. NORAD; the big tunnel complex under the mountain from which they be plannin' to fight World War III if it ever goes down. Huge walls of blinkenlights, 30-foot-thick blast doors, "We could tell you, sir, but then we'd have to kill you", the whole weird trip. Cornpone accents with their fingers on the pulse of the Apocalypse.

Oh, \*man\*, I said to myself. I have to talk to this woman. I haven't forgotten the nationwide media flap after \_War\_Games\_ came out. You remember, that silly movie where the kid with the voice-controlled IMSAI (snort) cracks into NORAD's computers and accidentally damn near starts a nuclear war? God damn; I'll bet the plot of that sucker is seared into the collective psyche of every security officer at Cheyenne Mountain, they probably screen the video every couple months just to keep the newbies on their toes.

What kind of hideous Federal heat could land on me if PAMELA D MILLER has hacker/cracker confusion on the brain? I imagine some steel-eyed amazon in a blue suit exuding grim determination to Nip This Menace In The Bud. \*Bad\* scene for a guy who is, after all, better known in some circles for practising witchcraft and stone anarchist-loony politics than for The Book. Yiiiii ... visions of sinister limos and Men In Black pulling up to my front porch. "We want to ask you a few questions, sir." So I called my editor Terri and Guy Steele (credited coauthor) and told them all the proceedings so far. Nervous laughter all around. Lugubrious jokes.

I need to convince this woman and her unknown masters that I'm a \*harmless\* lunatic. Time to track PAMELA D to her lair. (Yes. Think of her that way, Pamela D., like one of those impossible anonymous synthetic blondes in an upscale skin magazine. "Well, I'm into sailing Sunfishes and I really like kids, you know?". Good. A \*much\* less threatening mental tableau.) I limber up my phoning fingers and call the number blazoned above her address.

<click> <sputter> "NORAD operator ten. What extension?"
Gulp. "Uh, I'm trying to reach Pamela D. Miller? I got a product
information query from her."

"Do you have an extension, sir?"

"Um, no I don't. Just this number. And her address." I reel it off. "Try the base locator at Peterson, sir. 554-4020."

"Thanks", I said, and hung up."

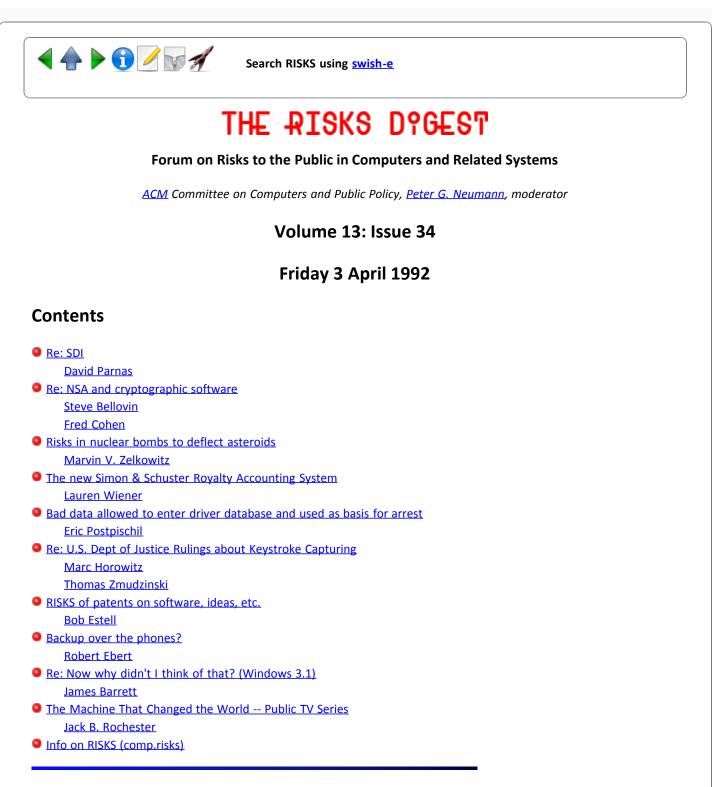
Ohhh-kay. NORAD for sure. Hail Eris! PAMELA D's hanging out somewhere under a couple of cubic miles of rock, likely in some cramped little office with 1950s-era furniture and walls painted institutional puke-green. And an old-style black phone. (How long has it been since you've seen a black phone?) (Trust me, this is what the military version of bureaucratic rabbit warrens looks like.) Or maybe at some gleaming console watching telemetry from all those KH-11s we're supposed to pretend don't exist. Hah. Heads up, Pammy; constructive chaos is about to enter your life. All hail Discordia!

This is about where things started to get really Kafkaesque. The base locator is their directory information desk. I ask for Pamela D. Miller's extension and get 3247 (remember that number). I call it. Some guy who sounds exactly like Andy Griffith answers: "



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# Ke: SDI (Newsweek, March 23,1992) (<u>RISKS-13.33</u>)

David Parnas <parnas@qusunt.eng.McMaster.CA> Thu, 2 Apr 92 16:07:28 EST

When I read that

"[The] Pentagon disagrees that deploying a spaceand ground-based defense system poses significant technical challenges. The complexity of the software required to coordinate Star Wars, for instance, is no more daunting than programs that control nuclear reactors, it says."

I certainly breathed a sigh of relief. Having had a look at both types of programmes, I am comforted by the impression that the Pentagon employee who stated that opinion had never seen either type of software. Dave Parnas

### NSA and cryptographic software

<smb@ulysses.att.com> Thu, 02 Apr 92 15:52:42 EST

The NSA and the Software Publishers' Association appear to have reached an agreement that would allow some exports of cryptographic software, as long as the keys are constrained to be sufficiently short. The net effect is a slight but potentially useful improvement over what was previously exportable.

Umm -- according to the NY Times article on the subject, things are actually a bit murkier. The details of the algorithm are supposed to be secret. (How long that will work is debatable, of course. In fact, it isn't even particularly debatable; I think we know the answer.) Naturally, a number of folks are quite upset about that aspect.

Now that NSA and RSA have come a little closer, we need to bring in BSA (the Boy Scouts of America). Be prepared! Imagine, a merit badge for cryptography?

Actually, they do have one. Or rather, Way Back When, the Cub Scouts had a something or other in cryptography. Being innocent of the distinction between a ``code'' and its key at the time (and for that matter, of the distinction between a code and a cipher), I persuaded the Powers That Were that I had fulfilled that requirement \*25\* times, by coming up with \*25\* different Caesar ciphers...

--Steve Bellovin

## Kisks of a national policy against good crypto

fc <FBCohen@DOCKMASTER.NCSC.MIL> Thu, 2 Apr 92 21:56 EST

Just an opinion - I think financial competitiveness is far more important than not being able to read crypto to the US at this time.

I can purchase an RSA on a smart card from Phillips in the EC, but I cannot sell a slower RSA for the PC to people in EC. What this seems to say is that they can have it, but I can't sell it to them - or in other words - they get the money from our research!!!

And then there is the old wire tapping thing. As far as I am concerned, it is the FBI's business to find a way to read my mail if they care to, but it is not my job to help them do it. That's why I use an RSA whenever I want to send something private.

Which brings me to the newest development at ASP. We have decided to do all further crypto development oversees. This is because if we do it here, it's against the law to export it, but if we do it there, we can still import it and sell it here. Any such policy, if it is to be effective, must also restrict import - otherwise, the financial motivations will move all crypto oversees. This is of course happening. Want an example?

At the 5th virus conference, the people from the EC cheered when they heard that virus defenses are export controlled. In my case, my EC competitors get a 6 week advantage over me in everything they do, because each new version has to go through paperwork at the US government that takes this long. As a result, I have moved my further virus defense development to the EC. They get the money in stead of the US getting it, but I get a smaller piece of a bigger pie, which earns me more money in the long run.

How long will it be before we give up the little leadership we have in information protection? Not long! All over the EC and in the far east and in Australia, there are research groups forming at universities for computer security researchers. They get funding and tenure, and even publish articles. In the US, there is lip service, and a few universities offer a course or two, but you cannot find more than 2 experts at any US university!

So I think the real risk is that in the name of maintaining national security, we are giving up our leadership in security!

Have a nice day - FC

#### Risks in nuclear bombs to deflect asteroids

Marvin V. Zelkowitz <mvz@cs.UMD.EDU> Thu, 2 Apr 92 17:13:01 -0500

I just listened to a local radio station talk show concerning proposals to use nuclear weapons to change the orbit of asteroids heading towards the earth, and while the discussion was factual, it poses a long term risk on science in this country. The discussion was by the radio commentator and a physicist from a local university. The general tone of the show and the facts presented were:

1. Neither took the threat very seriously and were very flippant about the whole process.

2. Rationale for such proposals seemed to be the large number of (unemployed?) nuclear scientists needing a new threat to work against since the Soviet threat is disappearing.

3. Congress held a hearing on the potential for such a collision with an asteroid.

4. NASA held two workshops to discuss this problem.

5. There is a non-zero probability of such a collision actually happening.

6. The last big collision of an asteroid with the earth was about 65 million years ago, anything that large is probably already known, we will have several near misses first before any collision, giving from several decades to several centuries advance warning before such a collision.

The risk here (besides the obvious one of having the earth blow up)? There is a lack of knowledge by the public on risks, safety, and the costs and tradeoffs of increasing safety (and decreasing risk), especially given the flippant tone of both radio commentators. It was probably reasonable for Congress to hold such a hearing since the potential damage would be catastrophic. It probably was reasonable for NASA to hold a workshop to discuss the risks of such a collision and potential solutions. Given the extremely small probability of such a collision and the high costs of preventing it, the process should have probably stopped there. However, it is important for the public (and scientists and Congress, even) to at least study such issues. The next time some issue like this comes up, there may be a tendency to dismiss it before there is any scientific discussion of its reality.

-- Marv Zelkowitz, Computer Science, University of Maryland, College Park mvz@cs.umd.edu

### **\*** the new Simon & Schuster Royalty Accounting System

Lauren Wiener <lauren@reed.edu> Thu, 02 Apr 92 15:29:18 -0800

I am writing a book about software bugs. Today I was working on a chapter featuring development disasters. The royalty statement for a previous book arrived. It is several days late, in a big envelope with a glossy brochure and a form letter that begins:

"Dear Author:

"We are very pleased to provide you with your royalty statement for the current period. This new statement is enhanced in form and content and is the initial statement generated by the recently implemented Simon & Schuster Royalty Accounting System."

The letter ends:

"Any major system implementation involves a transition and refinement period. We anticipate that you may have issues that require attention, and we are prepared to address your concerns in an expeditious manner.

If you have any questions, please call our Royalty Department toll free number..."

The check is made out to Lauren Carter. Carter? From Wiener? How did they do that? It's not even close!

I called the toll-free number. A human -- an agreeable and intelligent one -- is still in the loop at 5:30 P.M. EST. He promises to straighten it out. But the first thing he says to me is, "You wouldn't believe how much they spent on this system!"

Sometimes life is too perfect.

[Look for Lauren's Trip Report on the panels and invited talks at SIGSOFT '91, which is just going to press in the ACM SIGSOFT Software Engineering Notes vol 17 no 2, April 1992. I probably already noted that the proceedings of that conference are out as SEN vol 16 no 5, December 1992. PGN]

#### Mean of the second s

Eric Postpischil <edp@being.enet.dec.com> Thu, 2 Apr 92 05:28:44 PST

Below is the full version of a letter I have sent to various agencies and representatives in New Hampshire. In summary, some person was stopped for traffic violations, and gave a false name and address and no other personal identification. The violations were unpaid and unchallenged and so were recorded in the given name without that person's knowledge. License suspension proceedings were initiated, but notice was sent to the false address since the Department of Safety had updated their computer records with the erroneous information. Eventually, the innocent person was stopped and arrested for driving without a license.

-- edp (Eric Postpischil)

. . . . . . . . . . . . . . . .

6 Hamlett Drive, Apt. 17 Nashua, NH 03062 2 April 1992

An open letter to the Department of Safety, police officers, judiciary, and legislative representatives of New Hampshire

Dear People:

A few months ago, an acquaintance of mine was stopped by a police officer for a traffic violation. According to a check of their driving record, their license had been suspended, so the officer arrested them. It turns out this person had been the victim of a fraud, and the Department of Safety, the police, and the courts made mistakes which compounded the consequences. The charges have been dropped and the Department of Safety records partially corrected, but court records remain in error, and there are lessons to be learned from this incident. (I will not name the victim here, but appropriate parties, such as officials who wish to correct records, can get this information by contacting

#### the author.)

Fraud occurred on three prior occasions, which the Department, the police, and the courts failed to catch. Some person was stopped for traffic violations. This person apparently did not present any identification to the police officer who stopped them, but they gave a misspelling of the victim's name as their own and gave the address of a relative of the victim as their own address. (According to New Hampshire statutes, a person stopped for a traffic violation need not have their license with them but is supposed to present their driver's license at the peace officer's office within 24 hours.)

On three occasions, this person must have failed to present identification within the allotted time, yet there was apparently no follow-up investigation by any of the officers involved. The records of the violations were sent to the Department of Safety, which accepted them as correct in spite of the fact that there was no physical evidence at all that the person owning the affected records was in fact the person at fault. The Department matched the misspelled name with that of our victim and updated their database with the new, incorrect address. The violations were placed in the victim's records. Further, proceedings were begun to suspend the victim's license.

Notices about the violations and the suspension proceedings were sent to the incorrect address, where it was ignored. It seems to me to have been unwise to ignore official letters rather than forward or return them. I guess that because they were arriving at the incorrect address, they might have been presumed to be spurious and unimportant. Regardless, the fact that they were ignored is not in any way the fault of the victim.

There are several lessons to be learned. It is improper to place damaging data in a person's record when there is no supporting evidence -- no record of violations should have been placed in the victim's record nor should any court have made a finding of guilt until there were actual physical evidence. There was no driver's license, no signature, no fingerprint, no match of vehicle records, no photograph, and no witness who knew the person. Even the police officers who made the stops could testify only that the person said they were the victim, not that they actually were. As a society, we must recognize that if we rely on databases to provide important information, then we are assuming a great risk if incorrect data enters the database. There must be rigid controls to allow only accurate information into the database. Without these controls, the database cannot be considered accurate, and it is wrong to rely on it. An insecure database is not a proper basis for making arrests or otherwise penalizing human beings.

Another lesson is that the Department and police officers should be wary of fraud. When a person fails to present proper identification within the allotted 24 hours, this must be followed up by investigation. It must not be followed up by mechanically completing the paperwork to record a violation. Justice requires evidence and due process, and mechanical processing of violations provides neither to our citizens. Further, when a person fails to present identification during a traffic stop, the officer should secure some other evidence of their identity, perhaps by taking a photograph for later examination.

Finally, there is a lesson to be learned about database records and privacy.

Although the Department of Safety keeps these records, we should not consider the Department to be the owner of the records. Each record is owned by the person whose record it is, and the owner has a right to know what is in the record and when changes are made. The owner has a right to control their record to ensure that it is accurate. In this incident, the Department accepted a change to the records without checking with the owner to verify the change. This is like a bank allowing anybody to walk in and sign a new signature card for your account and then letting the person withdraw funds from your account. That is a serious flaw. Whenever any change is made to a person's record, the Department should send a complete notice to that person. When the change includes an address change, the notice should be sent to the former address.

I would also like to add that I am appalled that any court, magistrate, or other judiciary official would make a finding of fault against a person not only without evidence but also without properly serving notice to that person at their true address. Such administration of traffic laws is a travesty that subverts basic principles of justice in this country.

There is one good note. After the arrest, a letter was sent to the Department of Safety requesting correction of the mistakes. The Department responded extremely quickly -- by phone the day after the letter was placed in the mail. This is typical of the wonderful service the Department usually provides; they are to be commended for doing an excellent job on the whole. I only hope the Department can provide the same quality of service in preventing mistakes like this from happening in the first place.

On the other hand, the Attorney General's office has not acted so responsibly. The victim has managed to identify the guilty person and locate a witness to the fraud, yet the Attorney General's office has refused to become involved.

#### Recommendations

I call upon the Department of Safety to rectify its record-keeping procedures so that records cannot be altered without the knowledge of their owner and that incorrect information is detected.

I call upon police officers to be wary of fraud, to follow up with investigation when identification is not presented, and to regard their statements on official documents and to courts as testimony. On this latter point, observe that a police officer who has not examined identification cannot truthfully testify that they witnessed a certain person committing a traffic offense. The most they can testify to is that they witnessed somebody claiming to be a certain person committing an offense, and this distinction should be made clear in all official documents and court testimony.

I call upon judiciary officials not to make any finding of fault unless there is physical evidence and to ensure that the rights of our citizens to due process and to confront their accusers are fully protected. In particular, no judiciary official should accept the presentation of a summons to an unidentified person as proper service of a summons. I call upon the elected representatives of our citizens to ensure that the above tasks are accomplished. This state and this country are sorely lacking in data protection laws. Every day, citizens become further bogged down in a morass of databases containing information about them they cannot examine, control, or correct. People are steadily losing the ability to control their own lives.

You, our representatives, must fix this. You must protect people from wrongdoing by faceless bureaucratic machinations, and you must ride herd on the enforcement and judiciary branches of our government to ensure that our rights to due process and fair trials are protected.

Sincerely, (signed) Eric Postpischil

## Ke: U.S. Dept of Justice Rulings about Keystroke Capturing

Marc Horowitz <marc@MIT.EDU> Thu, 02 Apr 92 12:24:18 EST

<> Unfortunately, correct. The situation is roughly analogous to having <> to post signs saying that there are TV cameras monitoring your condo.

I must be misunderstanding you. The building I'm in (the student center at MIT) has a bank branch and a grocery store. Both have cameras, and neither have signs announcing them, I just checked. Neither conceal their cameras. Is a condo special?

Very true. For example, an "alleged penetrator" (prosecuting attorneys >> prefer to avoid the H(acker) word as "too warm and fuzzy") was monitored >> while committing (what I'd consider to be) electronic breaking and entry. <> He got off because he hadn't been warned that he was being monitored.

So, if someone breaks into my house, and I managed to follow him around, and watch him steal stuff, is that information not admissible in court because I never tapped him on the shoulder and said "don't mind me, I'm just watching you"? Should I have a sign on my apartment announcing that "By entering these premises, you consent to the possibility that the owner might actually watch you and file charges if you are breaking and entering."?

Marc

### M In-Re: Re: U.S. Dept of Justice Rulings about Keystroke Capturing

"zmudzinski, thomas" <ZMUDZINSKIT@UVAX6.DISA.MIL> 2 Apr 92 15:22:00 EST

DEFENSE INFORMATION SYSTEMS AGENCY

Dept: DNSO/DISM Tel No: 703 285 5459 (DSN) 356 Subject: In-Re: Re: U.S. Dept of Justice Rulings about Keystroke Captu

Apparently my dry wit was a tad too desiccated, sorry. Condos \_do\_ have some special laws (a condo fee isn't rent nor is it a mortgage payment), but surveillance isn't one of them.

I was giving a deliberately absurd, but all too real, example. There \_ARE\_ legal requirements relative to surveillance; what depends on where you are and what/who you're "surveillancing" (if "there ain't no word that can't be verbed", then such verbs can certainly be gerunded, right?).

Here, you may have a vacation-behind-bars-ish requirement to post such a sign; there, there may be no LEGAL requirement, but you post a warning to get a better return on your effort and scare off the badguys; (and everywhere, the Communication Cops want to get into your knickers?).

> So, if someone breaks into my house, and I managed to follow him ...

If you do as you said, it's your word against his, and assuming he left no physical evidence, I doubt that you'd even get the case to court. Of course, if you made the alleged burglar so nervous that he tripped on the throw-rug, \_YOU\_ could be prosecuted under the anti-"deathtrap" laws. (You did know that you can't leave a deadfall inside your doorway, didn't you?) By the way, I wrote "prosecuted", not "convicted", but the way that juries are "instructed" these days, I wouldn't rule it out.

> Should I have a sign on my apartment ... >

Given the current crazy state of our laws, it wouldn't hurt. Let me point out that I didn't write this mess!

### KISKS of patents on software, ideas, etc.

"FIDLER::ESTELL" <ESTELL%FIDLER.decnet@scfb.nwc.navy.mil> 2 Apr 92 16:02:00 PST

I guess I'm getting cranky in my old age (54). But I grow weary of the energetic youngsters (regardless of age) who want to patent every new toy - even if it ain't new! Like "...the first ever machine independent benchmarks..." hyped in one computer magazine; turned out they were NOT comparable between PC's and Mac's, nor DOS and UNIX-like hosts; i.e., one could not compare results, to help in a purchase decision. NOW \*that's\* REAL independence! (Not to mention that I was doing machine independent benchmarks in 1967-68.)

Apple's claims about "look and feel" of the icon/mouse interface should be faced down, in federal court, by a consortium of IBM, AT&T, H-P, etc. who graciously concede the icon/mouse interface to Apple - IF (and only if) Apple will abandon the keyboard and command line interface, on the ground that the plaintifs (IBM et al) got there first. Imagine using any computer, without a keyboard, and without command lines, even short ones - like single characters. Pretty tough.

Now, I'm not picking on Apple. (I use a Mac II.) It's just that their "look and feel" suit has gotten more press than most others. Squelching it once and for all might make other frivolous suits more rare.

Bob

### Mackup over the phones?

<Robert\_Ebert.OsBU\_North@xerox.com> Thu, 2 Apr 1992 11:07:48 PST

Excerpted from TidBITS#114/01-Apr-92, source: BackData, info@backdata.com

[Discussion of problems with existing backup systems deleted. People either don't do them or don't do them well.]

So the BackData guys realized that the best possible option is for all the data on your hard disk to be backed up automatically at night to another physical place. Short of hiring elves, the only way to do this is via modem, but with some of the current highspeed modems and sophisticated pieces of software out there, they figured that it would be possible with a bunch of Macs and a lot of storage devices.

....In terms of software, you just need AppleTalk Remote Access and Retrospect 1.3, which can back up any volume mounted on its desktop.

I haven't tried this yet, but the theory is that at some point in the middle of the night one of their backup Macs calls your Mac (which had better be on). A simple macro ensures that all your volumes are mounted read-only on their systems, and then Retrospect goes to work, backing up only the files that have changed according to specific selectors that you set up previously. This allows you to avoid backing up your System file all the time, even though it will almost always be marked as modified whether or not you've added any fonts or sounds. Once the backup is done, another macro copies the catalog file to your hard disk (so you can see what was backed up), dismounts your volumes, and disconnects the modems to finish the process.

Retrieval is a slightly stickier issue. Essentially, the process works in reverse, with one important exception. You call them and make sure your DAT tape is in the drive of a Mac at a certain phone number. After your Mac calls the storage Mac, you then run Retrospect over the remote connection....

I expressed some doubt about the reliability of cobbling together these off-the-shelf programs, and the BackData folks admitted that they're in the process of writing several dedicated programs that will automate the process much more cleanly, one for DOS and one for the Mac. Their programs didn't sound as though they'd be as flexible as Retrospect, but would work much more cleanly over the phone lines, especially with restoring data. Interesting concept this, and one which could eventually go national with an 800 number. It's basically a form of insurance, but one which could save a lot of important data in the event of disaster.

[Summary of costs deleted. Initial startup fee (includes hardware) and hourly connect fee during backups.]

The risks are numerous. Among them: granting "late night" dial-in access to home and office PC file systems, physical and electronic security at the remote site, authorization for backup restores, and backup data being held by a commercial company that lives on profits and is vulnerable to bankruptcy or hostile takeover.

--Bob (bebert.osbu\_north@xerox.com)

## Ke: Now why didn't I think of that? (Windows 3.1)

James Barrett <barrett@holly.gatech.edu> Thu, 2 Apr 1992 06:42:54 GMT

Also, Windows 3.1 has been touted as "eliminates UAEs!!!" Of course, it does this by renaming them to be something else...

James C. Barrett (barrett@cc.gatech.edu) Georgia Tech College of Computing

## Public TV Series

"Jack B. Rochester" <0002757498@mcimail.com> Fri, 3 Apr 92 15:43 GMT

I saw Bob Frankston at the coming-out party for PBS's new series, "The Machine that Changed the World" that begins next Monday, and we both thought you should consider posting it to the Risks Forum. Perhaps it is risky not to see how our industry is being popularized for the mass media. In any event, credit for the following -- this was passed on to me by my brother, who works at DEC. P.S. Another risk: the title of the series is the same as that of a recent book about the \_auto\_.

PBS COMPUTER SERIES

The Machine That Changed The World

On Monday evening, April 6, 1992 at 9:00 PM EST, and on successive Mondays until May 4, PBS will present "The Machine that Changed the World," 5 programs on the history of the electronic computer and its impact on society.

Produced by WGBH Boston (makers of NOVA) and the BBC, and with major funding

provided by ACM and Unisys, the series highlights the fifty year revolution in computing and information technology -- a revolution that is still going on.

Beginning with World War II research and the ENIAC, which was co-invented by J. Presper Eckert and the late John Mauchly (a founder of ACM). "The Machine that Changed the World" follows the unpredictable course of information technology from the room sized data processing centers of the 1960's to desktop personal computers of the 1980's to virtual reality of the 1990's, describing events that have altered society in profound and totally unexpected ways.

Check your local PBS listings for broadcast times on the following Monday evenings:

o April 6 - "Giant Brains", covers the wartime events that led to the 1946 debut of ENIAC, the world's first general purpose electronic computer.

o April 13 - "Inventing the Future", examines how the computer rose from obscurity to become the engine that powers business throughout the world.

o April 20 - "The Paperback Computer", explores how computers became small, affordable and easy to use.

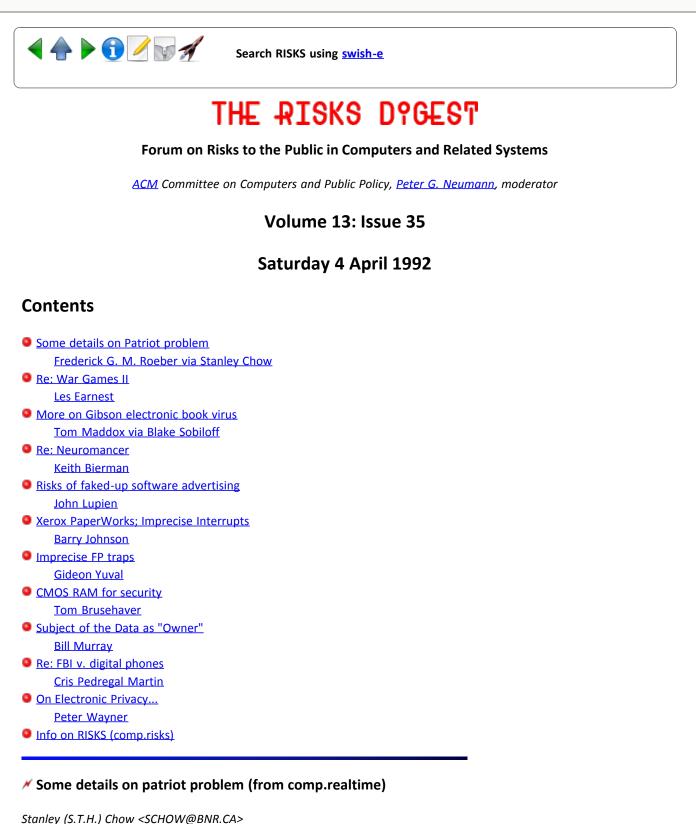
o April 27 - "The Thinking Machine", focuses on the most ambitious goal of all - creating a computer that will vie with humans in intelligence.

o May 4 - "The World at Your Fingertips" looks at the social revolution wrought by computers - and the price we pay.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



3 Apr 92 17:58:00 EST

This is the first time I have seen a detailed description of theround-off/accumulation problem.Stanley Chow(613) 763-2831

Article 74 of comp.realtime: Path: bqnes23!bmerh2!bnrgate!stl!uknet!mcsun!dxcern!vxcrna.cern.ch!roeber From: roeber@vxcrna.cern.ch Newsgroups: comp.realtime Subject: Re: Design question about Patriot Message-ID: <1992Apr3.104714.1@vxcrna.cern.ch> Date: 3 Apr 92 09:47:14 GMT References: <11204@mindlink.bc.ca> <1992Apr3.062551.7306@sequent.com> Sender: news@dxcern.cern.ch (USENET News System)

In article <1992Apr3.062551.7306@sequent.com>, jjb@sequent.com (Jeff Berkowitz) > [...]

> The article states "...this particular Patriot battery had been
> running continuously for about 100 hours...[and]...had built up
> a timing lag of 0.3433 second." This timing error was sufficient
> to shift the "range gate" enough to cause the system to disregard
> the Scud.

>

> My "comp.realtime" question: what algorithm in the Patriot system
 > would cause an ABSOLUTE time variation like this to change a
 > relative computation, like the predicted course of the incoming
 > missile?

I just received my copy of the US General Accounting Office's "Report to the Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives: Patriot Missile Defense -Software Problem Led to System Failure at Dhahran, Saudi Arabia" (phew!)

Since I can't find a copyright notice on it anywhere, I'll quote the appropriate paragraph:

"The range gate's prediction of where the Scud will next appear is a function of the Scud's known velocity and the time of the last radar detection. Velocity is a real number that can be expressed as a whole number and a decimal (e.g., 3750.2563...miles per hour). Time is kept continuously by the system's internal clock in tenths of seconds but is expressed as an integer or whole number (e.g., 32, 33, 34...). The longer the system has been running, the larger the number representing time. To predict where the Scud will next appear, both time and velocity must be expressed as real numbers. Because of the way the Patriot computer performs its calculations and the fact that its registers are only 24 bits long, the conversion of time from an integer to a real number cannot be any more precise than 24 bits. This conversion results in a loss of precision causing a less accurate time calculation. The effect of this inaccuracy on the range gate's calculation is directly proportional to the target's velocity and the length of the the system has been running. Consequently, performing the conversion after the Patriot has been running continuously for extended periods causes the range gate to shift away from the center of the target, making it less likely that the target, in this case a Scud, will be successfully intercepted."

Interestingly, when the Israelies were running their Patriot systems, they studied the heck out of them, and noticed this problem after merely 8 hours of operation. (8 hours corresponds to a range-gate shift of 55 meters; 100 hours corresponds to 678 meters.) They sent this data back, and the Americans responded with something like, "This was designed for the European theater, where it would be run for a few hours before being moved. Who in his right

mind would run a system continuously for eight hours? Or more?" They did write a software patch to fix the problem, but it took two weeks to arrive in Saudi, because of transport difficulties. It arrived the day after the failure.

Frederick G. M. Roeber | CERN -- European Center for Nuclear Research e-mail: roeber@cern.ch or roeber@caltech.edu | work: +41 22 767 31 80 r-mail: CERN/PPE, 1211 Geneva 23, Switzerland | home: +33 50 42 19 44

### War Games II (Raymond, <u>RISKS-13.33</u>)

Les Earnest <les@sail.stanford.edu> Thu, 2 Apr 92 20:28:47 -0800

I found Eric Raymond's account of NORAD telephone indirection amusing but not at all unusual -- I recently encountered a more elaborate runaround in dealing with the county bureaucracy that manages the bus system here. Eric is lucky that he did not get the treatment that we used when I had an office at C.I.A. headquarters. There we answered the phone with "Hello" and, unless the calling party immediately named a person who shared the office, we were programmed to hang up without another word.

As one who helped design the initial computer system that went into the Cheyenne Mountain facility, and who much later provided some input to the screenwriters who wrote "War Games," I will assert that there is less there than meets the eye (and imagination). That facility was intended to integrate and control a number of other so-called command- control-communication (C3) systems, but suffered from the same fundamental design flaws as its predecessors. (See my C3 series in RISKS that I suspended two years ago, but that I intend to resume as soon as I get time.)

Let me acknowledge that the Cheyenne Mountain facility is not totally useless. If a nuclear holocaust does occur and if the evironmental security systems there function as advertised, the residents of that hole may have an opportunity to repopulate the Earth after a time.

Fortunately, the even more elaborate and senseless proposal to develop a successor system, dubbed the Strategic Defense Initiative by Ronald Reagan, now seems to be fading away despite attempts to revive it as a Killer Meteorite Initiative.

Les Earnest, 12769 Dianne Drive, Los Altos Hills, CA 94022 415 941-3984 Les@cs.Stanford.edu ...decwrl!cs.Stanford.edu!Les

### More on Gibson electronic book virus (from alt.cyberpunk)

Blake Sobiloff, Human-Computer Interaction Lab <ccb@rac2.wam.umd.edu> Fri, 3 Apr 1992 02:53:26 -0500

Subject: Re: William Gibson's next novel.... From: tmaddox@milton.u.washington.edu (Tom Maddox) Date: 2 Apr 92 19:29:44 GMT Organization: The Evergreen State College, Olympia, Washington Newsgroups: alt.cyberpunk,rec.arts.sf.written References: <1992Mar31.231258.4312@pasteur.Berkeley.EDU> <D+g+aNC@engin.umich.edu> Keywords: William Gibson Xref: umd5 alt.cyberpunk:9967 rec.arts.sf.written:6007 Sender: news@u.washington.edu (USENET News System) Path: umd5!haven.umd.edu!darwin.sura.net!jvnc.net!yale.edu!spool.mu.edu!uwm.edu!ogicse!henson!news.u.washington.edu!milton.

Message-ID: <1992Apr2.192944.9444@u.washington.edu>

Given the recent confusion (mine included) about a few matters Gibsonian, I thought I might post a clarification. I talked to him last night, and he said:

the virus-loaded thingie does or will soon exist, but it's certainly not his next novel; in fact, it's a couple of thousand words that he refers to as "the text," and it's poetry, accompanying "a bronze booklike object" that weighs a bunch and contains etchings by Dennis Ashbaugh and a diskette with the Gibson poem;

the poem, if the software works the way it's intended to, will self-destruct after a single reading ("but you can videotape it");

this is all aimed at the art collector's market, and I get the impression Gibson's part in it occurred as a favor to the artist;

in re the draft dodger matter--he was never actually drafted but went to Canada to evade the possibility; he says he would not claim the moral credit that goes with being an actual draft dodger.

This report brought to you by Citizens for More Accurate Cyberfacts.

Tom Maddox, tmaddox@u.washington.edu

## Ke: Neuromancer (<u>RISKS-13.33</u>)

Keith Bierman fpgroup <Keith.Bierman@eng.sun.com> Thu, 2 Apr 92 15:06:07 PST

>William Gibson, well known for his "Neuromancer" (which in 1986 anticipated >what is today known as virtual reality), has a new book, ...

Gibson was far from the first. The details are best left to the rec.sci.fi.\* groups; but it is serious revisitionst history to claim that Gibson is the creator of VR.

[Gibson's new Book of the Dead might be titled NECROMANCER, to contrast it with his earlier NEUROMANCER! PGN]

# Kisks of faked-up software advertising

John Lupien <lupienj@hpwarq.wal.hp.com> Fri, 20 Mar 92 15:14:23 EST

Brian Kantor's article about the zip codes being wrong on the addresses used in an advertisement for a text processing package brought to mind another faked-up advertisement that is potentially much RISKier - in COMPUTER LANGUAGE there is a recurring advertisement for a software product that uses a compound bow with an arrow as its illustration. Perhaps the intent is to indicate that the product is high-tech, accurate, powerful, and easy to use (all of which might be said of compound bows), but if you look closely you notice that the arrow is on the wrong side of the bow, and could not possibly be actually nocked on the bowstring. If the bow was loosed in this configuration, the most likely result would be embarrassment on the part of the operator, but if the arrow were to partially catch the string, it could do considerable damage to the operator and/or anyone else around. The target, however, would not be exposed to significant risk of being hit... and if I was the intended target of the advertisement, I have to say that it was rather wide of the mark...

To put the risk more succinctly, it is important to get the details right in your advertisements: people who notice lack of attention to detail in advertisements may well assume that this is indicative of the product as well.

John R. Lupien, lupienj@hpwarq.hp.com

### Xerox PaperWorks; Imprecise Interrupts

BARRY JOHNSON <WB15471@ibrdvax1.bitnet> Fri, 3 Apr 92 09:38:00 EST

I had assumed a couple of recent items would have been answered by someone more informed than I but, since they haven't, let me offer my bit ...

Security v. Xerox Corp.'s PaperWorks

The March 30, 1992 issue of \_InfoWorld\_ (p.37) shows the top couple of inches of the form that one uses to request stuff. Right below a 'Please do not write above this line' header is a SECURITY block. It has 26 boxes across the page with a letter A-Z above each. Soo, there is something ...

#### Imprecise Interrupts

As surprised as I was to hear that DEC's ALPHA chip may not return an interrupt tagged to the instruction that caused it, I was even more concerned by the subsequent discussion that seemed to imply that, since an IBM mainframe did this years ago, it is probably OK. As far as I know, the Unisys (Burroughs) A Series has been pipelining in its higher-performance machines for years but it has always reported an interrupt against the instruction that caused it. This is despite, I believe, the possibility that it may have over a dozen instructions concurrently in the pipe.

Not being a hardware person, I am left wondering: is it possible to properly manage inter-instruction dependencies in the pipeline without being able to track an interrupt to the instruction that caused it? Wouldn't it be necessary to track the offender so that one could determine the dependent instructions that will also need to be cleaned out? The bottom line is that just because it has been done before doesn't mean it is OK to keep doing it (c.f. MicroSoft Windows 3.1: just because NOT checking parameters has been done before doesn't mean they should keep doing it!).

Barry Johnson

## // Imprecise FP traps (Klossner, <u>RISKS-13.27</u>)

Gideon Yuval 1.1114 x4941 <gideony@microsoft.com> Fri, 1 Mar 92 13:04:40 PST

In <u>RISKS-13.27</u>, andrew@frip.wv.tek.com says "the only practical difference between precise & imprecise exceptions is that you can't report the PC of the offending instruction when imprecise". I think this is overoptimistic:

To implement the default (denormalizing) mode of IEEE754/854 underflow handling, most systems trap on underflow, and let the trap-handler do the denormalizing. This becomes difficult in an imprecise-exception environment, when the original operands may already have been overwritten by the time the exception occurs (even if the "offending" instruction can be determined).

Since a system that breaks IEEE defaults is obviously one that breaks IEEE, this seems a real issue.

Gideon Yuval, gideony@microsoft.com, 206-882-8080 (fax:-883-8101;TWX:160520) Microsoft, 1 Microsoft Way, Redmond, WA 98052-6399 (home: -232-2119)

### CMOS RAM for security

Tom B. <intran!clam!tom@uunet.UU.NET> Fri, 3 Apr 92 09:49:18 CST

Over the past 5 years our little division has used the Premis accounting software package. About 3 years ago, Xerox bought our company, and has kind of left us be our own little company. We continued to use Premis software.

Last fall Xerox started cutting back, and was thinking of rolling our accounting into Xerox's accounting, so we stopped paying support to Premis for the software we were about to stop using. Changes happen and our office moved. During the move, the accounting PC lost its battery that saves the cmos ram (its an original IBM AT). Once I found what drive type it had, and reset the date and time, and got everything running, the accounting guy tried his software. Well the software now says we are not licensed.

Thinking a simple phone call was all that it would take to get the license going again, the Premis folks informed us there would be a fee, including all the months of support we didn't pay for, but were still using (their assumption). Then when pressed, they claimed the software license was "non-transferable", and since Xerox is now our company name, the software must be re-licensed (Xerox had been sending them checks for most of 3 years, and they never complained).

A more wizardly PC guy who works here looked at things, and found the Premis software was on its own non-DOS partition, and the original Premis floppies only contained a DOS program that can load this non-DOS partition. The backup procedures used here only backup DOS partitions (Premis charges extra for the backup program, so someone decided we would use our own backup program).

Maybe these aren't risks, but they sure are dangerous to people not computer wizards, in that no one had informed anyone that this was really special software (non-DOS), using non-standard hardware (cmos ram), in ways not intended. What if some new piece of software had needed the same cmos ram to store its license.

Tom Brusehaver uunet!intran!tom

## Subject of the Data as "Owner" (Postpischil, <u>RISKS-13.34</u>)

<WHMurray@DOCKMASTER.NCSC.MIL> Sat, 4 Apr 92 18:04 EST

>Finally, there is a lesson to be learned about database records and privacy.
>Although the Department of Safety keeps these records, we should not consider
>the Department to be the owner of the records. Each record is owned by the
>person whose record it is, and the owner has a right to know what is in the
>record and when changes are made. The owner has a right to control their...

It is a gross over-simplification to assert that because a record is about me that I "own" it. While I clearly have an interest in it, and while the holder may have a responsibility to me to protect that interest, that interest may be far short of ownership.

Ownership may be defined as the exclusive right to use. This is the definition that we usually have in mind when we talk about chattels. With regard to real property, such ownership may be granted by the sovereign and subject to eminent domain, but the definition still works reasonably well. Ownership of information is similar in that most of my rights, for example copyrights, are granted by the sovereign or the legislature. Information is different in that some use of it by others may not infringe my rights or intent.

However, if we were to use this definition of ownership and if we assert that that ownership automatically or by default rests with the data subject, then we would expect that all use of personal data would have to be by delegation of the subject owner's rights. Clearly this is not the case and the driving license record and the driving license itself are good examples to prove the point.

If under this definition I were the owner of my driving license record,

then the state would be able to use it only under a license from me. Clearly that is not the case. The record and its uses are authorized by law. It is kept at state expense for a legitimate state purpose. While some state laws do make explicit mention of the rights of the subject of the data, most are silent. None suggest that the state uses the record at the sufferance of the subject.

Other examples are less clear. A copy of the pay record is kept by the the employer to fulfill his legal obligations to the employee, the employee's bargaining agent, the state, and the owners; many of these obligations he could not meet in the absence of such records. They are kept at his expense for a legitimate purpose. While it may well be that his right to keep such records is granted by the employee as part of the employment agreement, I am not aware of any such agreement that speaks explicitly to the issue. Perhaps more to the point, I am not aware of any challenges to the rights of employers to keep such records.

While equity and fair information practice both clearly suggest that the employee has a protectable interest in the record, such interest would appear to be far short of "the exclusive right to use."

Balancing the rights and interests of record keepers against the rights of record subjects is a complex issue. It will eventually be clarified, and perhaps even codified, at law. To date the law is mostly silent. In the presence of such silence I suppose anyone can assert what he would like to be the outcome as though it were fait accompli. I would suggest that it is less than helpful, perhaps even destructive, to do so.

William Hugh Murray, 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL

## Ke: FBI v. digital phones (Dobkin, <u>RISKS 13.33</u>)

<pedregal%unreal@cs.umass.edu> Fri, 3 Apr 92 9:49:01 EST

Daniel Dobkin offers a justification for the FBI's reasons to demand an ability to wiretap without Telco cooperation. (This follows the reasoning by Brian Kantor, carefully avoiding its disputed last step.) Dobkin says:

> In fairness to the FBI, there are other possibilities, such as when a
 > Telco employee is himself the subject of an investigation.

I find this extremely naive. If to investigate a Telco employee one must stay outside of Telco COs and such, there is a serious security problem at Telco regardless of other technical issues. The other side of the coin (misuses of such capabilities) has been discussed already.

I agree with Kantor that any conceivable (legal) wiretap can be carried out with Telco's cooperation. This is enough, and it has been well argued that more than this (i.e., what the Bureau demands) poses risks both on civil rights and technical perspectives.

The risks of the good-natured remark by Dobkin are the assigning of (pure) "motivation" or moral qualities to (in this case, government) institutions, and forgetting Occam's razor: Telco wiretapping is sufficient, effective, and cheap. Why more?

Cris Pedregal Martin -- Computer Science Dept., UMass, Amherst.

#### ✓ On Electronic Privacy…

Peter Wayner <wayner@cs.cornell.edu> Sat, 28 Mar 92 10:12:57 -0500

I read William Session's piece in the NYT on why the FBI wants to maintain the ability to tap phones and I think he makes good points. If we want to defend cryptography and electronic privacy, I think we need to argue that privacy is not just a philosophical shield used by child pornographers and drug dealers. It is an essential tool that normal people need to protect their interests. I wrote this down in an op-ed piece on Senate Bill 266 (the one that would ban encryption) that didn't see light. Rather than re-invent the squeal, I'll just send it along.

Everyone knows the problem with postcards. The mailman hands over the mail and says, ``Too bad about your brother. Paid all that money to go to ski in Switzerland just to break his arm on the first day.'' Right now, the Senate is considering an anti-crime bill that effectively requires all communication to be as easily readable to government officials as postcards. The reason, they say, is that drug dealers and other criminals are using secret codes to do business. The sad truth is that the bill will hardly deter criminals. If anything it will make their lives easier by making it impossible for American companies and citizens to keep anything confidential.

The point of Section 2201 of Senate Bill 266 is to prevent people from using secret codes. The practice is not widespread now because people communicate with paper and sealed envelopes are enough to do the trick. In the coming years more and more letters and documents will travel electronically and in electronic communication, encryption is the equivalent of an envelope. Although you can't write sealed with a kiss across it, you can make still make sure that no electronic postmaster is perusing your love letters. There may be no seal, but the banks and other businesses can use encryption to keep financial statements confidential.

Although the language of the bill makes it more a non-binding resolution than a real law with teeth, it specifically asks that all manufacturers of communication equipment ensure that the ``plaintext" of a message is easily available to the state. No one knows what this will entail, but there is the real danger that the executive branch might make regulations based on these non-binding wishes of Congress. In any case, any piece of communication that can be read by the government can also be read by 16 year old hackers or more importantly, foreigners companies spying on their American competitors.

The problem, in the eyes of the bill's authors, is that computers make it too

easy to jumble a letter or a ledger record into incomprehensible mess of seemingly random noise. Only the person with the correct password can resurrect the file. The government is worried that this computer power will be a tremendous hindrance to investigations. They won't be able to find produce any evidence of wrongdoing because everything will be encrypted in code.

While this may be a problem, it's nothing new. Criminals have been using secret codes since the beginning of time. One of the classic cliches of Hollywood is the doublespeak of gangsters. One asks, ``Did the shipment of tomatoes come in yet?'' The other responds, ``Yes, and they will cost you 10,000 bananas.'' Henry Wadsworth Longfellow made the encryption technology of the American revolution famous when he set it to rhyme. ``One if by land, two if by sea, and I on the opposite shore shall be.'' Although there weren't any computers involved, the message got through.

It is easy to create an innocuous system that doesn't look like a code. When a major New York jeweler was caught evading sales tax by sending empty boxes to addresses out of the state, the police found that they were making a little dot next to the illegal entries in the books. When Elliot Ness brought Al Capone down for tax evasion, he got the bookkeeper to decipher the cryptic entries in the books. Would prohibiting encryption stop this behavior? Hardly. What's another law when you're already taking on the IRS?

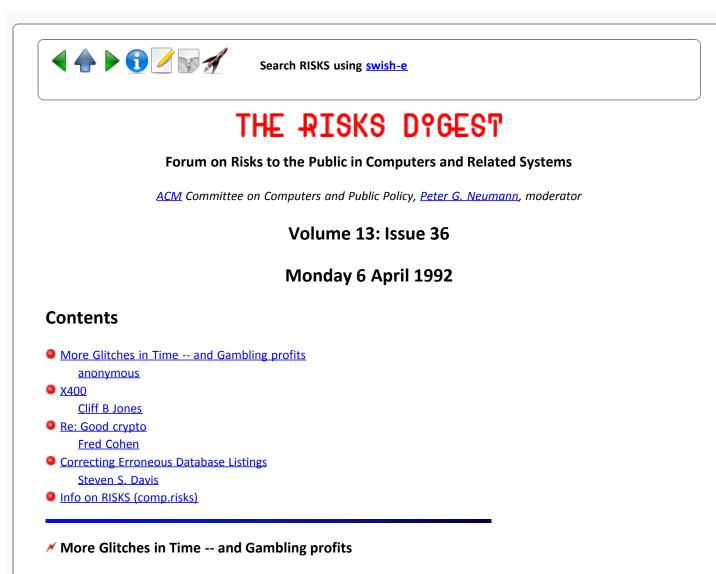
Almost by definition, this bill will touch sensitive subjects. If people consider something a private matter, they usually have a reason for feeling that way. There may not be a right to privacy specified in the constitution, but many feel that there should be strict limitations on the bounds of government. In a sense, requiring all messages to travel on the equivalent of postcards isn't much different from getting a search warrant for every envelope in the country.

But, the people on the other side of the spectrum who feel that ``privacy'' is just a philosophical shield for suspicious activity should be just as wary of the bill. Criminals are notorious for using confidential data to defraud. My credit card company assumes that if I tell them my account number and the billing address over the phone then I am probably who I say I am. But when every bill or letter must be readable by the government, who knows which criminal will find a way to discover my credit card number and billing address? Companies won't be able to protect themselves or their customers with encryption.

This bill should alarm any business with trade secrets. Encryption is to computers what locks are to filing cabinets and security guards to the front door. The Soviet Union, France and Iraq, to name just a few, already devote a substantial effort to stealing American non-military technology. It doesn't make sense to prevent business from protecting themselves.

The fact is that individual people are the best guardians of their own information. Privacy is not just an important legal tradition-- it is also a good crime deterrent. The police will always dream of listening to the hidden thoughts of the criminals, but gaining the ability to scan every letter in the country won't make a difference. Even the stupidest crooks know enough to not to spell out their plans on a postcard. The rest of us who have completely legal secrets, though, will be left with no protection by Senate Bill 266.





<[anonymous]> Mon, 6 Apr 92 12:37:12 xDT

This being daylight savings day, a programmer down the hall at another firm and I got onto a discussion of time related programming errors. He related two very interesting real-life errors that I thought you all would be interested in.

Both of these programming failures were discovered when he worked at a race and sports book (ie gambling hall). These both happened in Las Vegas, and the names and places are not being posted to protect the guilty from shame. :-) For those not familiar with how sports books work:

Basically the book takes bets on sporting events, and horse / dog races. Bets are PLACED up to a particular point (usually start time), at which time that event is CLOSED. After the event is over, the winner is POSTED. Bets are then paid based on the posted winner. The computers (of course), have safety features to prevent you from placing a bet after an event is closed. The closing and posting is done by a single person, who spends all day watching 6 or 7 TV's. Of course, the system keeps an "accurate" audit trail with regard to the times that items are entered. At a local book they were using a system that was designed for horse races, but instead they were using it for dog races. Now Nevada law says that betting stops when the first horse enters the gate (minutes before the race is over), but dog races are not closed until a few seconds before the gate opens. Dog races are also fast, taking ~30 seconds. The difference in time span is crucial, because the system originally only recorded the time in HH:MM, since seconds were not crucial for a long horse race. Because of this, a race could close, start, and be posted, all within the same minute. This meant that you could sometime place a bet after the game was over, and the computer would still accept the bet. (REAL MONEY)

At another book, the employees managed to cheat the system for about three months. It was obvious to the auditing department that some cheating was going on, but all the computer records were clean, but it was equally obvious that everyone on the floor was ripping the book off. They way it worked was this:

When a game started in New York at 7PM (ATLANTIC COAST TIME), they would close the game at 7PM (PACIFIC COAST TIME). Everybody in accounting assumed that the computer tracked the times in the proper time zone for that game, because that's how the employees were using it.

Eventually someone asked one of the programmers, and found out that all times were supposed to be in local time, and well.....

P.S. The book that discovered these two bugs never bothered to report them to any of the other books using the same software. :-(

#### 🗡 X400

Cliff B Jones <cliff@computer-science.manchester.ac.uk> Sun, 5 Apr 92 15:35:11 BST

I have recently run into a problem with the X400 protocol that could I believe kill e-mail as we know it. Remember when messages used to be conveniently queued? Well, if the X400 is "congested" it sends a (long) rejection message (which does \*not\* include the original message!) back to the originator. Just imagine a conventional mailing service where the delivery man who has too much to carry just sends back a note saying "I threw your mail in the trash".

I also understand that the whole problem comes from charging arrangements between PTT's - no one want to pay for storage so reject the messages when busy, don't send them back (but remember to charge for the rejection message).

I'd love to be corrected on this! If I'm right, e-mail could just die. I've already given up using it other than at weekends from here to Germany.

cliff jones

\* Re: Good crypto [risks of posting risks to RISKS] (Cohen, <u>RISKS-13.34</u>)

# fc <FBCohen@DOCKMASTER.NCSC.MIL> Sun, 5 Apr 92 20:21 EDT

My computer must be slow ... I still haven't gotten a copy of the risks posting I made several days ago, but I've gotten several computer mail postings from around the world about the posting. I guess information posted to risks gets to the EC before the US.

Yes [to a query], you can print what I said in risks elsewhere, but I can't imagine why you would want to.

Someone in the EC thought (I think) that I was complaining about the EC's policy. Not so. I was complaining about the US policy that you can't export the DES or RSA, even though you can buy it cheaply everywhere you have to get approval for export. There's even a public domain version of the DES (source in C) widely available in the US. (I would post it on risks, but I'm afraid that risks might then export it). It seems that US law permits me to publish my source code for the RSA and export that, and if you have a scanner, you can read it into your computer legally.

I think I am now leaning toward publishing the illegal-to distribute portion of my system on paper and shipping it in the manual. Then you only have to type in the expression (defun encode (x) (mexpt x e n)) to implement the RSA on your system. After all, it is legal to sell software that does very fast modular exponentiation with unlimited precision! if the default version of encode is (defun encode (x) x), it doesn't violate US law because it doesn't encrypt!!

As to doing the development in Israel, I understand you can get very inexpensive mathematical expertise in Israel, and according to recent rumors, you can sell in volume to China from there, but on the other hand, the total effort of developing the cryptosystems requires only a few hours of relatively non-expert programming time. You can still do the theory in the US and export it on paper.

By the way, the source code for one of the cryptosystems I am not allowed to export without permission was published in Computers and Security (the IFIP journal), so I understand that my competitors are using the algorithm already. I guess it's alright to have my competitors sell my cryptosystem in the rest of the world as long as I can't.

Fred

## Correcting Erroneous Database Listings

Steven S. Davis <paa1338@dpsc.dla.mil> Mon Apr 6 13:05:24 1992

In the article "Bad data allowed to enter driver database and used as basis for arrest" in <u>RISKS-13.34</u>, Eric Postpischil described the problems that resulted when public officials put false data into their databases. The problem of false data finding its way into interacting databases and spreading throughout them and becoming hard to completely eliminate, as you don't even know all the

places it may have reached, is already real, and can be expected to get worse. Mr. Postpischil correctly indicates that a person should be reviewed as the owner of his or her data in a public database and be advised of changes and able to make corrections. However, the public databases are only a tiny fraction of those containing records on you. Most of them are private, the owners regard the information as proprietary, and would never accept the expense of notifying the subjects of changes. So what can be done to protect people from bad data ?

The answer that I would propose for consideration is that the great nightmare of science fiction, an authoritative official database, may be in fact the only way to protect ourselves from all the little brothers spreading information about us. If an such an authoritative database existed, any other database that used information on you that was contradicted by the authoritative database would expose it's owners to liability. They would therefore have to assure that before any data was used it would be checked against the central database. If some bad data was circulating about you, it could be stopped with one update to the central record, and if that failed, you would have a clear case of negligence, and a much better chance of collecting damages if the falsehoods did you any harm.

I don't propose that this database list all the facts about you, though some people might prefer that it carry very complete data. It would include only a)the information that you gave it, and b) information that was placed there as the result of a contract, court case, or other legal action. The subject of the data would have full access to the information and the right to require corrections. There would probably be a fee involved for each piece of information posted ( usually paid by the subject, though in some cases by others or by public agencies, and possibly only covering a certain period of time ), but corrections would be free. It would generally only involve data you need to protect yourself from falsehoods. In most cases this would only involve offering appropriate identification of oneself and documentation of the data, but when facts are disputed the entry might require a court to decide the facts and authorize the change.

I've no firm idea on how such a thing would be set up. I don't expect it soon, because of the cost and because of continuing fears of such centralized information. But as there is already a massive amount of decentralized information about us out there, the owners of which are not accountable to us though they can have devastating impacts on us, it seems to me that a centralized, accountable record is a desirable thing, and that the lack of one puts us more at risk than the creation of one.

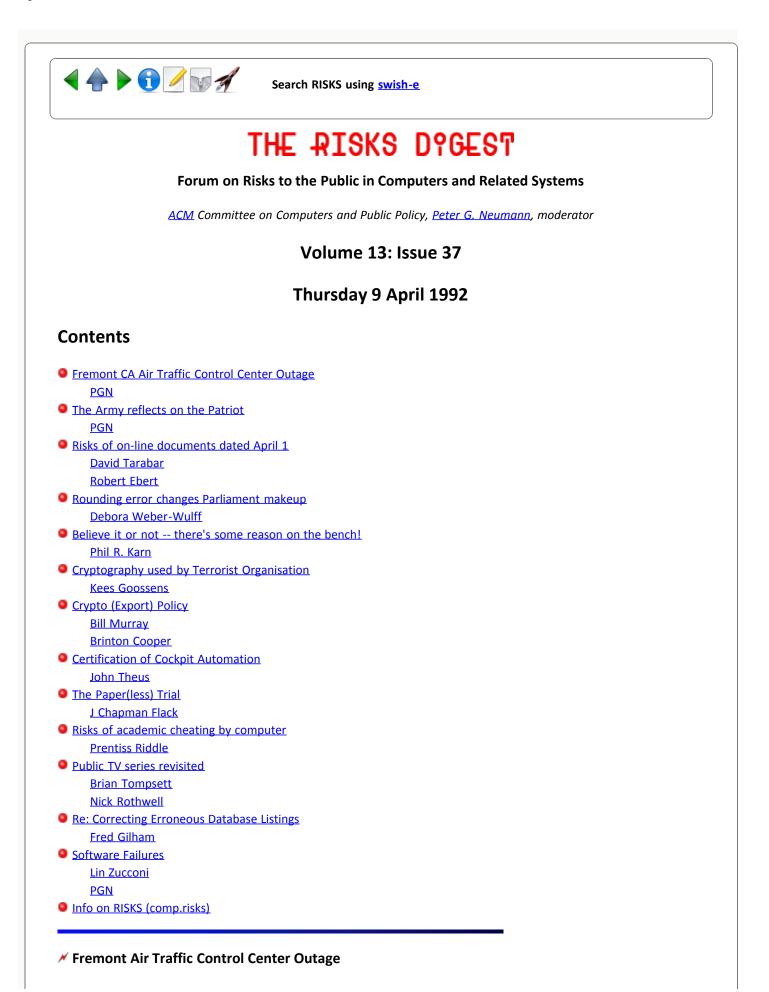
[The silly parts of the above opinions are wholely my own; any intelligence that crept in was probably borrowed. None of it reflects the position of my employer. Steven S. Davis (ssdavis@dpsc.dla.mil)]



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 13: Issue 36



# "Peter G. Neumann" <neumann@csl.sri.com> Thu, 9 Apr 92 10:07:14 PDT

While I was in the air back to SFO from Washington yesterday morning, the Oakland CA en-route traffic control in Fremont had a major snafu, seriously snarling West-coast and Pacific Ocean air traffic from 8:40am PDT, for two hours. Outgoing flights were delayed more than incoming flights. The backup system requires manual handshaking where otherwise the system would handle handoffs automatically, so there was some element of risk involved. However, the outage of the one center did not directly impact safety. Required separations between planes were increased to 20 miles for landings and departures, instead of 3 miles, and the net effect was a return to leisurely pace of the 1950s. The cause of the failure is not yet known, although it was thought to be a software problem. [Some details can be found in, Traffic Control Center Failure Snarls Airline Flights, By Jack Viets, San Francisco Chronicle, 9 April 1992, front page]

### Mathematication The Army reflects on the Patriot

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 9 Apr 92 11:41:06 PDT

The Army acknowledged on 7 April 1992 that its glowing claims of success were based on faulty data and indicated it is now certain that the missile ``killed'' roughly 10 Iraqi Scud warheads out of more than 80 fired at Israel and Saudi Arabia, although the actual number could be greater.

[Source: A front-page article by George Lardner in the Washington Post, Army Cuts Claims of Patriot Success: Reduced Figures on Missile's Precision During Gulf War Are Issued, 8 Apr 1992.]

Also, see the earlier item on MIT Professor Theodore A. Postol's article and its aftermath, discussed in <u>RISKS-13.32</u>. Postol was on Fox TV early on the morning of the 7th, prior to the Army briefing, discussing the Patriots. He suggested that 10% was much closer than the 80% previously claimed, and that is actually conceivable that NO direct kills were actually achieved!]

## Kisks of on-line documents dated April 1

David Tarabar <dtarabar@hstbme.mit.edu> Wed, 8 Apr 92 19:31:02 -0400

In <u>Risks 13.34</u>, an article describing an alleged remote backup service, began:

- > Date: Thu, 2 Apr 1992 11:07:48 PST
- > From: Robert\_Ebert.OsBU\_North@xerox.com
- > Subject: Backup over the phones?
- > Excerpted from TidBITS#114/01-Apr-92, source: BackData, info@backdata.com

The article mentioned some of the obvious risks involved and subsequent

issues of Risks contained follow-up articles.

However, in TidBITS#115, the author mentioned that TidBITS#114 was the April Fools issue and all of the content was fictional.

Not getting an April Fools joke might be more of a risk in on-line documents because often they are not read until some time after the first of April. (Of course there can be a similar problem with hard copy media - I get several magazines whose April issue arrives in late February or early March.)

David Tarabar (dtarabar@hstbme.mit.edu)

# Kisks of too-subtle April Fools Jokes (Backup over the phones?)

<bebert.osbu\_north@xerox.com> Tue, 7 Apr 1992 14:03:01 PDT

<u>RISKS-13.34</u> (Friday 3 April 1992) carried a submission from me forwarded from TidBITS#114/01-Apr-92 about Backing up Macs and PC's over the phone.

TidBITS#115/06-Apr-92 carried the following notice:

To quote from the excellent movie "Spinal Tap," "it's a fine line between clever and stupid." I may have fallen off that fine line in writing TidBITS#114, because despite a few clues and hints, the fact that it was indeed our annual April Fools issue appears to have gone generally unnoticed. Almost everything in that issue was false - though often entirely possible and even intensely desirable - with the exception of the IBM marketing move (which was strange enough to be an April Fools joke), and the Dolch projection panel (which I used to make the last article more believable). Sorry folks, if I threw you for a loop.

So, there you have it. I don't consider myself to be terribly gullible, but I was taken in. [I didn't have this problem with any other April jokes... I don't think. But then, most of the ones I got were substantially more obviously jokes than this. Xerox is \*not\* going to lease it's newly acquired buildings in Palo Alto to the Mariott hotel chain, and an "Amusement park for Silicon Valley geeks" requiring "magnetic badges built into pocket protectors" is \*not\* going to be opened on the neighboring land at Page Mill & Foothills.]

In any case, apologies all around for spreading what turned out to be false information. The backup scheme described seems entirely plausible, and even lucrative. Looking over the rest of the TidBITS digest, I suppose there are clues to be had... in retrospect. In comparison to the rest of the silliness that the rest of the net goes through every April, TidBITS was the height of subtlety. Ah, well, whatever it takes to relieve those tax-time blues, I suppose.

The IBM marketing move (from TidBITS#114/01-Apr-92): Ralph Amundesen wrote with some interesting information about IBM. Evidently, IBM is so worried about OS/2 that the company has expanded its battalion of salesbots by drafting the entire company. I don't know if this will go as far as dark-suited IBM folks out pounding the pavement ("Excuse me, Ma'am, may I come in and demonstrate what OS/2 2.0 can do for you today?"), but all 344,000 employees are in it for fun and prizes. It's a step up from grade school, but IBM employees could win medals, IBM software, IBM hardware, or even cold hard cash. I sure hope they don't stop in here since I don't have 30 MB free under SoftPC to test it. Sheesh, wouldn't you think it would be easier to just buy a few TV spots like Microsoft is doing?

The Dolch projection panel (from TidBITS#114/01-Apr-92): Interestingly, Dolch Computer Systems just released a color LCD projection panel that can double as a stand-alone screen for a mere \$8500.

--Bob (bebert.osbu\_north@xerox.com)

### Kounding error changes Parliament makeup

Debora Weber-Wulff <weberwu@inf.fu-berlin.de> Tue, 7 Apr 1992 12:38:29 GMT

We experienced a shattering computer error during a German election this past Sunday (5 April). The elections to the parliament for the state of Schleswig-Holstein were affected.

German elections are quite complicated to calculate. First, there is the 5% clause: no party with less than 5% of the vote may be seated in parliament. All the votes for this party are lost. Seats are distributed by direct vote and by list. All persons winning a precinct vote (i.e. having more votes than any other candidate in the precinct) are seated. Then a complicated system (often D'Hondt, now they have newer systems) is invoked that seats persons from the party lists according to the proportion of the votes for each party. Often quite a number of extra seats (and office space and salaries) are necessary so that the seat distribution reflects the vote percentages each party got.

On Sunday the votes were being counted, and it looked like the Green party was hanging on by their teeth to a vote percentage of exactly 5%. This meant that the Social Democrats (SPD) could not have anyone from their list seated, which was most unfortunate, as the candidate for minister president was number one on the list, and the SPD won all precincts: no extra seats needed.

After midnight (and after the election results were published) someone discovered that the Greens actually only had 4,97% of the vote. The program that prints out the percentages only uses one place after the decimal, and had \*rounded the count up\* to 5%! This software had been used for \*years\*, and no one had thought to turn off the rounding at this very critical (and IMHO very undemocratic) region!

So 4,97% of the votes were thrown away, the seats were recalculated, the SPD got to seat one person from the list, and now have a one seat majority in the parliament. And the newspapers are clucking about the "computers" making such a mistake.

Debora Weber-Wulff, Institut fuer Informatik, Nestorstr. 8-9, D-W-1000 Berlin 31 dww@inf.fu-berlin.de +49 30 89691 124

## Melieve it or not -- there's some reason on the bench!

Phil R. Karn <karn@thumper.bellcore.com> Tue, 7 Apr 92 19:18:33 EDT

Defense Loses Bid to Present Animated Videotape Depicting Baton Blow By Linda Deutsch, Associated Press Writer

Simi Valley, Calif. (AP) The judge in the trial of four officers accused of beating a motorist refused Tuesday to let jurors see an expert witness's animated videotape recreating the first baton blow. Superior Court Judge Stanley Weisberg said he wasn't convinced that the tape, created by a biomechanical engineer with the help of a computer program, was scientifically reliable. ``It would lead the jury to think it must be accurate ... that it's true because the computer shows it,'' Weisberg said. ``Just because it's sold in software stores doesn't make it reliable.'' However, the judge said the witness, biomechanical engineer Carley Ward, could testify on the limited issue of how much force is produced when a baton strikes a human head and how much damage would be done.

Officers Theodore Briseno, 39, Laurence Powell, 29, Timothy Wind, 31, and Sgt. Stacey Koon, 41, are on trial in the March 3, 1991 beating of Rodney King. A bystander's videotape of the beating led to a nationwide furor over police brutality and inflamed racial tensions in Los Angeles. King is black, the officers are white.

Ms. Ward testified outside the jury's presence that Powell, in a test conducted by her, exerted 1,500 pounds of pressure when swinging a baton in a ``full power swing.'' Prosecution witnesses have said he struck King's head in such a manner.

If King was struck with that force, Ms. Ward said, she would have expected more injury than the broken facial bones he suffered. She said her experiments striking the heads of cadavers at such velocity produced brain injuries.

Michael Stone, Powell's lawyer, said he would need time to determine if he wanted to call Ms. Ward, given the limitations imposed by Weisberg.

### Cryptography used by Terrorist Organisation

<kgg@dcs.edinburgh.ac.uk> Mon, 6 Apr 92 10:10:08 BST

In <u>RISKS-13.34</u> various people wrote about cryptography. The following shows how it already used by terrorists. On Saturday 4th April the British newspaper the Guardian reported that all the leaders of the Basque separatist organisation ETA had been captured in a police raid in France. (ETA is a terrorist organisation in Basque, Spain which want independence from Spain. They have killed many over the last 10 years.) The leaders must have found out several minutes before the raid, as they tried to find matches to burn documents they had in their possession. Failing, they torn them up and flushed them down the toilet instead. (It is not stated whether the police recovered them.) The interesting part however, is that the police captured a computer (PC or laptop) from the ETA some time ago (more than 18 months if I remember correctly) but they have, to date, not been able break the code which was used to decrypt all the information. I suppose this must be a worst case scenario for intelligence organisations such as the police etc.

Kees Goossens, LFCS, Dept. of Computer Science JANET: kgg@uk.ac.ed.dcs University of Edinburgh, Scotland UUCP: ..!mcsun!ukc!dcs!kgg

## Crypto (Export) Policy (Cohen, <u>RISKS-13.36</u>)

<WHMurray@DOCKMASTER.NCSC.MIL> Tue, 7 Apr 92 07:50 EDT

The US policy on export of crypto, while silly, is not quite as silly as Fred thinks. He thinks that it is silly to discourage export of pure information in one form while tolerating it in another. In fact, that is not quite true.

While once embargoed, (indeed NSA asserted that mere discussions of crypto were "born classified") publication of cryptographic information is sufficiently like protected speech for its prohibition to raise constitutional issues. (You and I would likely agree that the law should not distinguish between the media of publication.) However, this is not the only reason that print publication is tolerated.

The government tolerates "publication" of crypto in hardware encapsulation because replication is very difficult. Likewise, the same information on paper appears to them to be safer than on machine readable media. While information printed on paper can be readily copied, the procedure must be in machine readable form before it can be used. While, as Dr. Cohen suggests, one can scan information from paper into a computer, the government sees this as undesirable but tolerable. This is only one of the silly parts of this policy.

Nonetheless, any use of crypto has the potential to increase the cost of intelligence gathering, and less important, reduce the effectiveness of law enforcement. While the government understands that it will not be completely successful, it believes that it has a responsibility to resist whenever and wherever it can.

History tells us that intelligence gathering is expensive in any case. It also tells us that we are better at gathering it than we are at using it. Nonetheless, it is a dangerous world. If you believe, with the government that cheap intelligence gathering is a high value, support the government policy.

The Director would have you believe that mere use of ISDN, much less secret codes, is inhibiting the ability of the government to enforce the laws against terrorism, drugs, and organized crime. If you believe that the use of commercial crypto by criminals is wide-spread, if you believe that law enforcement should be cheap and easy, and if you believe that law and order are values that are superior to individual freedom and privacy, then support the government policy. Otherwise, resist it.

If you believe that international electronically mediated trade and commerce require codes that both parties can trust, then you may wish to join FBC in resisting this silly policy. If you believe that international trade and commerce are more important than efficient intelligence gathering, then to the extent that you believe that, you have an obligation to resist.

William Hugh Murray, 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL

## Ke: Good crypto (Cohen, <u>RISKS-13.34</u>)]

Brinton Cooper <abc@BRL.MIL> Tue, 7 Apr 92 14:55:50 EDT

FBCohen@DOCKMASTER.NCSC.MIL has posted comprehensive criticisms of US policy regarding export of cryptosystems. In a word or two, he shows how absurd it is that an American could develop a cryptosystem abroad and both sell it both abroad and import it to the US without violating US export laws.

Surely spooks from NSA, FBI, CIA, Commerce, and others (Oops, does Commerce have spooks? It wouldn't surprise me) read Risks-Digest. Why, then don't we have an authoritative, or at least an informed rebuttal to his postings? Is this, after all, a partisan political decision that has not been made on the bases of what's best for US competitiveness but but rather of what best fulfills some hidden agenda?

C'mon, someone, speak up!

\_Brint

## Certification of Cockpit Automation

John Theus <john@theus.rain.com> Fri, 03 Apr 92 00:14:49 -0800

The 23 March 1992 issue of Aviation Week focused on automated cockpits with 9 articles on the subject. Very interesting reading. The most interesting quotes were in the article "Pilots, Human Factors Specialists Urge Better Man-Machine Cockpit Interface".

Near the end of the piece, Anthony J. Broderick, associate FAA administrator of regulation and certification is quoted several times. Quoting AW&ST:

Although there are "no real, fundamental changes needed" to certify advanced hardware and software under development by major airframe manufactures, there is a need "to develop procedures that will establish certification standards for a level of safety" when using such systems, he said. .... The agency's [FAA] experience base, in addition to rules established by the RTCA -formerly know as the Radio Technical Commission for Aeronautics -- that governs design standards for software and hardware used in automation equipment, provides an acceptable means to certifying systems as they are developed, according to Broderick.

Glad to know we don't need to worry about this anymore!

John Theus john@theus.rain.com TheUs Group

### Mathematical The Paper (less) Trial

j chapman flack <chap@art-sy.detroit.mi.us> Tue, 07 Apr 92 01:54:24 GMT

>From \_The Cincinnati Enquirer\_, date missing from my copy:

A judge's distaste for clutter is pushing Cincinnati's federal court into the high-tech world.

When a securities case comes to trial soon in the courtroom of federal district Judge Carl Rubin, reams of exhibits will be computerized and displayed on eight computer monitors.

The alternative is rows of cumbersome file cabinets lining the walnut-paneled walls of his courtroom for weeks on end. "And I hate that," he said.

...

...

...

With the push of a few buttons, the courtroom deputy can display the exhibits on three color monitors in front of the jury box, and on screens stationed before the judge's bench, witness stand and lawyers' tables and podium.

Computerization also may cut down on trial time because lawyers can change exhibits without carting posters and papers around the courtroom.

[The newspaper photo shows a monitor displaying the front and back of a bank check, signatures and all. "I saw it on the computer, so it had to be real...."]

Chap Flack chap@art-sy.detroit.mi.us

### Kisks of academic cheating by computer

Prentiss Riddle <riddle@hounix.org> Thu, 9 Apr 92 9:21:08 CDT

There is an academic cheating brouhaha this semester at the university where I work which is brimming over with computer risks. I am not privy to the details of the case, but here is a summary from the published accounts.

This university has an Honor Code governing student cheating which is a source of much school pride. Students agree not to give or receive aid on schoolwork and as a result the university can function without the burden of proctored exams. Alleged violations of the Honor Code are taken before the Honor Council, an elected student body which has the authority to dole out substantial punishments. Honor Council cases are publicized in the form of anonymous abstracts which mask the identities of all parties.

Enter the computer: Earlier this semester, two students were accused of colluding on a homework assignment which was done and handed in via one of the university's academic computer networks. Their TA noticed that portions of the two students' homework were identical, down to the initials of one of the students. Network officials were asked to examine backup tapes for the period of time in question and produced evidence which supported the theory that "Student B" had sent homework to "Student A" by electronic mail immediately before Student A turned it in. The students argued that they were innocent and were the victims of a frame-up by an unknown "User X" who they alleged had gained access to their accounts. The Honor Council refused to accept the "User X" theory and convicted both students. Student B's conviction was later overturned partly on the basis of further evidence supplied by network officials which suggested that Student A committed the acts of cheating alone by logging in to Student B's account.

Although officially the case is closed, it is the subject of much heated debate in the student newspaper and local Usenet newsgroups at the university. Both students continue to maintain their innocence and their supporters have rallied around the slogan "Free Student A".

Computer risks seem to surround this case on all sides. A few which come to mind:

-- The risk of cheating by computer in the first place. While academic cheating is as old as academia, the computer can make it, like so many other things, easier than ever before.

-- The risk of frame-ups. While the Honor Council appears to be satisfied that the computer evidence substantiates real cheating in this case, it is clear that a person with access to one or more users' accounts could at least cause them a major nuisance and possibly succeed in framing them of cheating. With the penalties involved going as high as academic suspension from a school which costs thousands of dollars per semester, this is no light matter.

-- The complexity of evidence in cases of computer cheating. Honor council members were quoted in the student paper as complaining about the new and bewildering kinds of evidence they are asked to consider in computer cheating cases, and critics of the Honor Council have complained about the dangers of being judged by people who are not users of the systems involved and don't thoroughly understand them.

-- The burden on system administrators. The network official who provided the bulk of the evidence estimated that he spent a full week gathering and analyzing it. Since the case came up, the local academic network has extended the period of time it keeps daily backups before recycling them. How much data is it reasonable to keep, and to pore over, in order to provide evidence in cases like this? I don't know of a way to determine a firm answer.

-- The danger to trust and to openness. Both the university's Honor Code and the tradition of open exchange of information within the computing community

are threatened by cases like this. Must students be kept in a "padded shell" to prevent computerized cheating?

-- Prentiss Riddle ("aprendiz de todo, maestro de nada") priddle@hounix.org

## Public TV series revisited

Brian Tompsett <bct@cs.hull.ac.uk> Mon, 6 Apr 92 11:08:18 BST

In <u>RISKS-13.34</u>, a new PBS series on computers was mentioned. These 5 programmes have already aired some weeks ago on the BBC in the UK. I have seen all 5 and regard them as excellent. Their coverage of the historical material was the most accurate and even handed I have ever seen. Their coverage of risks issues is also exemplary. I could seriously use them in undergraduate teaching and did not regard them in any way as "technopulp" for the masses.

There is the probability that some of the programmes are "tailored" to the home audience. I have experienced this before with other WGBH/BBC co-productions. This highlights some interesting assumptions often made with regard to TV programmes. If the programmes are in our field we assume them to be "technology for the masses", whereas the masses, having seen it on TV assume the fact presented in the program to be true. Further, if the programme is aired around the globe, or around the nation from more than one TV station we assume everyone shares the same programme we do.

Do they tell the people in Cambridge (either one) that they invented the computer and at the same time tell someone in another time zone that it was invented by a little old lady from Novosibirsk? Are we being manipulated by global telecasting on an Orwellian scale? Who can tell? Not easy is it.

Brian Tompsett, University of Hull, UK.

### Machine that Changed the World

Nick Rothwell <nick@dcs.edinburgh.ac.uk> Mon, 6 Apr 1992 13:45:42 +0000

>Perhaps it is risky not to see how our >industry is being popularized for the mass media.

Perhaps, but I've seen three out of the five programmes and was quite impressed with the factual accuracy.

>Another risk: the title of the series is the same as that of a recent book >about the \_auto\_.

Erm, the Americans must be using a different name. Over here the TV series was called "The Dream Machine."

Nick.

# **K** Re: Correcting Erroneous Database Listings (Davis, <u>RISKS-13.36</u>)

Fred Gilham <gilham@csl.sri.com> Mon, 6 Apr 92 13:57:21 -0700

> The answer that I would propose for consideration is that the great
 > nightmare of science fiction, an authoritative official database, may be in
 > fact the only way to protect ourselves from all the little brothers spreading
 > information shout way

> information about us.

I disagree with this, or rather, think it should be an extremely last resort. I think promulgation of inaccurate information should be legally treated as a form of libel, with legal recourse for those who do it. Currently I understand that there is very little legal recourse for someone who suffers from inaccurate information in this manner, and so little incentive to eliminate it.

-Fred Gilham gilham@csl.sri.com

## 🗡 Software Failures

"Lin Zucconi" <lin\_zucconi@lccmail.ocf.llnl.gov> 7 Apr 92 16:24:42 U

Has anyone heard of or have evidence of a failure in a safety-related or other critical or security system where the developers claim they "did it right", e.g. they used good software engineering practices during development and had a good SQA program, and in particular, where they have identified common-mode failures in N-way redundant systems in hardware or software?

Lin Zucconi zucconi@llnl.gov

## Software Failures

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 9 Apr 92 11:00:10 PDT

Lin, You might look at the following paper:

\* Peter G. Neumann. The Computer-Related Risk of the Year: Weak Links and Correlated Events. Proceedings of COMPASS '91. IEEE 91CH3033-8, pp.5-8. This paper notes the 1980 ARPANET collapse, the 1990 AT&T long-distance collapse, and a bunch of telephone system outages, and considers seemingly weak-link failures that actually arose because of multiple-fault modes. It also notes the some further references that might be useful to you.

 S.S. Brilliant, J.C. Knight, N.G. Leveson. Analysis of Faults in an N-Version Software Experiment. IEEE Trans. on Software Engineering, Feb 1990, pp.238-247.

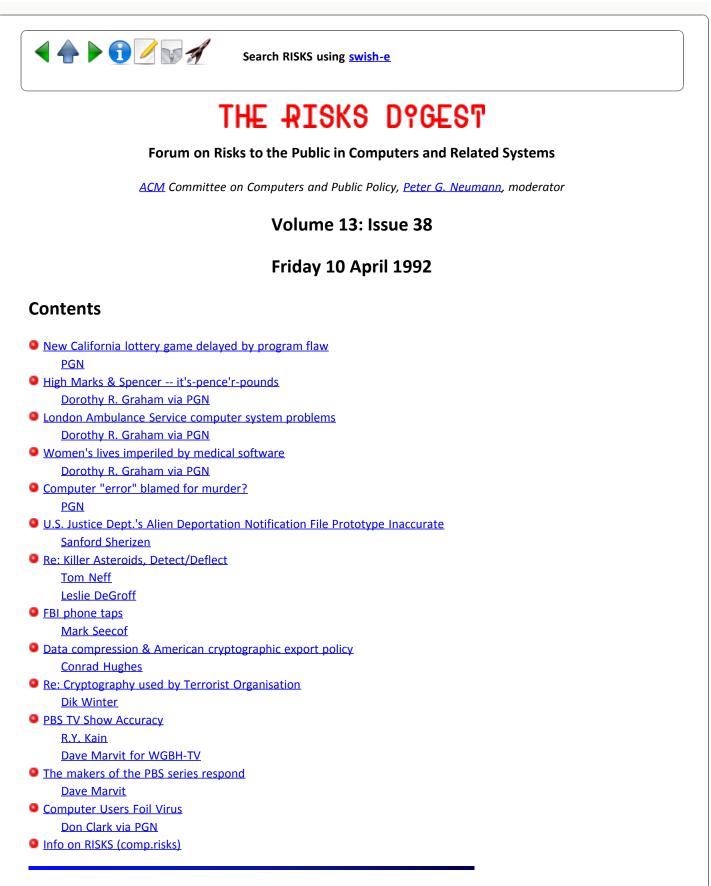
- J.E. Brunelle and D.E. Eckhardt. Fault-Tolerant Software: Experiment with the SIFT Operating System. AIAA Computers in Aerospace V Conference, October, 1985, pp.355-360.
- R.I. Cook. Reflections on a telephone cable severed near Chicago. SEN, 16, 1, pp.14-16.
- J. DeTreville. A Cautionary Tale. SEN, 16, 2, Apr 1990.

and look through the RISKS and Software Engineering Notes archives (index in Jan 1992). I imagine some of our readers will also send you further references, with CC: to RISKS, please.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# New California lottery game delayed by program flaw

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Apr 92 10:07:08 PDT The new `Daily 3' numbers game slated to begin today in California was postponed at the last moment by state officials concerned that the game might have been unfair. The problem was discovered only on Wednesday (8 Apr 1992), and diagnosed the following day. The final test indicated that the quick-pick pseudorandom number generating algorithm was biased. After a quick-fix programming change, the game is now scheduled to start next Monday. [Source: San Francisco Chronicle, 10 Apr 1992, p.A21]

[I suppose this will inspire a new research area -- Byzantine Pseudorandom Number Generators, in which 3n+1 PNGs are required to guarantee correct behavior in spite of n malicious or arbitrarily malfunctioning PNGs.
I heard on 1 Apr 1992 that Les Lamport has been asked to apply to the State of California for a research grant on this topic. But he was skiing (or Byzantining?) in Nevada. PNG -- oops, I mean PGN]

## High Marks & Spencer -- it's-pence'r-pounds

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Apr 92 13:35:50 PDT

Marks & Spencer is looking for the cause of an embarrassing glitch in systems at its shop in Paris which led to customers being massively overcharged. The retailer's Visa credit card transaction system added two zeros to 300 customer's bills so that a 1 pound pork pie cost 100 pounds. Marks' barcode and receipt printing systems were not faulty.

[Source: a clipping from Computing, 21 Nov 1991, contributed by Dorothy R. Graham of Grove Consultants, Cheshire, UK.]

## ✓ London Ambulance Service computer system problems

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Apr 92 14:01:26 PDT

London Ambulance Service continues to have software problems with its emergency dispatch system. The new 1.1M-puond system (being developed by Datatrak and Systems Options, with Apricot hardware) crashed on its first training session. Last year, an earlier system failed two major tests, and was scuttled; the Service sued the vendor (BT subsidiary IAL) and subcontractor (CGS). That system had costs escalate from 2.5M pounds to 7.5M pounds, and was supposed to have been ready in the summer of 1990. Another system for south London's nonemergency calls crashed in its first week, in April 1991.

[Source: An article by Jason Hobby in the Computer Weekly, 5 Dec 1991]

On 7 Feb 1992, an operator inadvertently switched off a screen, losing four emergency calls. On one occasion, the details of a call were lost; the caller called again half an hour later and was told that the details had been lost (by the computer), and an ambulance was dispatched. The patient later died, although ``it is not proven that there was any link between the delay and the

death."

[Source: An article by Jason Hobby in the Computer Weekly, 20 Feb 1992]

[Both articles were contributed to RISKS by Dorothy R. Graham, Cheshire, UK]

#### Women's lives imperiled by medical software

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Apr 92 14:08:05 PDT

The National Audit Office has issued a report blaming ``unreliable computer data'' for failing to identify high-risk groups of women being screened for cervical and breast cancer, which reduces the chances of successful scanning, and so contributes to the deaths of 15,000 women in England each year. The software is developed by Family Practitioner Services in Exeter. The report is now up for review by a Parliament select committee.

[Source: Article by David Evans, Computer Weekly, 20 Feb 1992, contributed by Dorothy R. Graham, Cheshire, UK]

### Computer "error" blamed for murder?

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Apr 92 10:02:40 PDT

Drug Offender Faces Murder Rap

#### PATERSON, N.J. (AP)

A drug offender under house arrest killed another man after a computer error enabled him to break his electronic anklet and leave the house, authorities say. Tony Palmer, a 21-year-old who had been serving a three-year sentence, was charged with fatally shooting Vernon Major, 19, last week.

The electronic surveillance system sets off an alarm if the prisoner moves more than 150 feet from a transmitter or breaks the bracelet or anklet. The alarm sounded and a printer in Trenton placed an asterisk by Palmer's name, but the information was not transmitted to a computer monitored by parole officers, Corrections Department spokesman Jim Stabile said Wednesday. The printout also is checked, but 700 names move constantly on that line, Stabile said.

## ✓ U.S. Justice Dept.'s Alien Deportation Notification File Prototype

Sanford Sherizen <0003965782@mcimail.com> Fri, 10 Apr 92 16:59 GMT

Inaccurate

The Department of Justice's Central Address File, which will be used to record and preserve the names and addresses of aliens and their representatives in

deportation proceedings, was reviewed by the General Accounting Office. The File is not yet fully implemented but initial reviews indicate problems. The General Accounting Office report (Jan. 23), covering a review of only four field offices, estimates that 22 percent of the records of the names and address of aliens involved in deportation proceedings were inaccurate. GAO believes that for ALL offices, some 12 percent of aliens may not be able to be notified about their deportation hearings due to inaccurate names and addresses under this system.

The Justice Department indicates plans to revise its current procedures. However, it isn't clear how they are going to achieve 100 percent accuracy in notification, which is essential when a deportation matter is at stake. Not appearing at a hearing can mean that individuals will lose their rights under the law, since it can and will be assumed that they were notified as required by law and/or did not let the authorities know when they moved. Recently, the U.S. has drastically (and often unfairly) restricted appeals and other protections in many deportation and political asylum cases. The result has been shameful incidents, including the deportation of Haitians who are now being threatened upon return to their country of origin. Data entry problems will simply reinforce those governmental decisions, resulting in automatic deportation orders when persons do not show up for their hearings. Reliance upon the computer as an essential part of this critical process \*without other forms of notification and review of agency procedures to ensure appropriate protection of applicants\* will cause great problems.

Sanford Sherizen, Data Security Systems, Inc., Natick, MASS

#### Ke: Killer Asteroids, Detect/Deflect

Tom Neff <tneff@bfmny0.bfm.com> 9 Apr 92 13:41:23 EDT (Thu)

For once, the New York Times had something intelligent to say on this matter in its lead editorial the other day. If astronomers are really convinced that the Earth-crossing asteroid impact threat is serious, would they be willing to take observing time away from other programs on \*existing\* instruments and devote it to the search? Oh, well maybe it's not THAT serious! :-) (The NYT stylebook forbids smilies, but if they ever used one, it would have been right there.) If the asteroid search is less important than anything telescopes are being used for now, the taxpayers might be forgiven for suspecting that this proposal has more to do with creating work and facilities for folks who've chosen to build their careers around space based interception issues than it does with a sensible and properly prioritized approach to protecting the planet.

The RISK here is our old favorite: institutional and career imperatives are capable of improperly driving public policy unless we keep a watchful eye out. Most people trust "astronomers" and "scientists" to tell us what is really important in that mysterious realm out there. When they trot out diagrams and photos, we naturally tend to accept their conclusions. But it ain't necessarily so. (I am not saying anything is fundamentally wrong with the process, though, since public inquiry like this very discussion tends to weed out errors.)

# Astroidal risks, minor core

Leslie DeGroff <DEGROFF@INTELLICORP.COM> Fri, 10 Apr 92 13:53:24 PDT

A minor correction might be in order on the posting about the problems and risks of "monitoring for astroidal risks".

The (widely believed) event of 65 million years ago was probably the last "stream clean most of the planet" size event, actual estimates of large (nuclear explosive level) collisions are for much smaller time scales such as a few thousand years apart for megaton size to once per million years for objects capable of devestating medium sized countries. Still hypothetical but with some evidence is that a medium sized sea strike triggered or contributed to ice age. There are a couple of examples of visible "smallish hits" in last few thousand years such as "Arizona's Meteor" crater. Of significance (and I am sure done a disservic by the media) it that one of the Nasa's proposals is simply to find and track these smaller but not harmless objects which are also of a scale that would be currenly feasible to deflect.

I don't recall the exact numbers but the explosive power of a meteorite (because of velocities range) range through equivalence in mass to power of high explosives.... as such a small objects of nickle iron are equivalent to lower nuclear range. A 20 meter chunk could be Hiroshima scale, a 100 meter chunk, megaton scale!!!!

Les DeGroff (degroff@intellicorp.com)

# FBI phone taps (Kantor, <u>RISKS-13.32</u>)

Mark Seecof <marks@capnet.latimes.com> Fri, 10 Apr 92 11:31:36 -0700

Like Brian Kantor (yo, dude) I'd be surprised to hear that there are many phones which can't be tapped at the end office switch. From reading the Sessions piece and other accounts I think what the FBI really wants is to place taps from their office in Washington (or perhaps from say, Colorado, to save on toll charges) so that they won't have to spend the staff effort to actually visit a CO. Instead, they'll just type a few keys and have the datastreams associated with calls from or to certain numbers duplicated and copied to their equipment. This capability will save them money and effort, reduce the chance that targets will learn about taps by suborning telco personnel, enable them to place many more taps, and just maybe increase the incidence of unlawful (warrantless) tapping. Of course, I am surprised that Sessions thinks the American people will want to pay higher phone bills in order to help the FBI tap their phones.

Mark Seecof <marks@latimes.com>

✓ Data compression & American cryptographic export policy

Conrad Hughes <chughes@maths.tcd.ie> Fri, 10 Apr 92 11:42:30 +0100

Could use of "non-standard" or uncommon compression techniques to facilitate high-speed data transmission also be undesireable for the NSA/FBI? Use of experimental/modified "coding" of data for purposes of compression could make data just as inaccessible as if it were encrypted for purposes of security.. Should we expect laws against use of non-standard data compression to succeed laws against data encryption?

On top of the patent problems related to data compression techniques, could this provide a killing blow for non-corporate research into coding/modelling?

(I may have used "compression" & "coding" in a slightly more interchangeable way than experts in the field would like - do not hesitate to correct me, but please accept my apologies in advance..)

Smail: Conrad Hughes, 42 Temple Road, Dublin 6, Ireland Email: chughes@maths.tcd.ie Voice: +353-1-976143

# Re: Cryptography used by Terrorist Organisation

Dik T. Winter <Dik.Winter@cwi.nl> 9 Apr 92 22:46:35 GMT

> the Guardian reported that all the leaders of the Basque separatist

> organisation ETA had been captured in a police raid in France. (ETA is a

> terrorist organisation in Basque, Spain which want independence from Spain.

A correction here. Basque country consists of three Spanish provinces and two French prefectures. The ETA wants to get all five in a independent country, but they are currently only active in Spain, although they take refuge in France.

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland dik@cwi.nl

# PBS TV Show Accuracy

faculty R. Y. Kain <kain@ee.umn.edu> Fri, 10 Apr 92 13:22:06 -0500

Seeing the praises for the TV series in RISKS, I must add that while what was shown was well done, I did notice that the one BIG OMISSION in the "conventional" histories of the business was also omitted from the show. That is the pioneering work in Iowa in the 1930s (about 1937) by Atanasoff, a physicist, who built a working machine that did perform calculations using vacuum tubes. I recall that he actually won a patent suit against Univac, which had been claiming patents on the basic idea of programmable (?) electronic computers. So why doesn't he get the credit that is his due? Perhaps he needed a better public relations department! Dick Kain (kain@ee.umn.edu) - EE Dept., University of Minnesota

## Ke: TV Show Accuracy]

WGBH-TV (Information Age) <wgbh@MEDIA-LAB.MEDIA.MIT.EDU> Fri, 10 Apr 92 18:17:28 EDT

Out of respect for John V. Atanasoff's efforts with the ABC Computer, "The Machine That Changed the World" has been very careful to avoid the term "first" in speaking of the ENIAC computer. Generally, we refer to it as the first "working" electronic computer.

However, the decision NOT to include Atanasoff's computer in the series was made only after a great deal of consideration. There is much debate about Atanasoff's machine -- did it ever really work?; could it be considered a "programmable, digital, computer" as we defined the computer for the purposes of our series?; how does one weigh the pronouncement of a judge against the opinion of the majority of the computer community (including historians) regarding Eckert and Mauchly's place in computer history versus Atanasoff's?

Ultimately, we came to the conclusion that the series (with its inevitable time constrictions) can only focus of those machines that influenced further development in the field. With that criteria, we could not justify spending the large amount of time that would have been necessary to tell the Atanasoff story. In addition, some authors claim that Mauchly "stole" the idea from Atanasoff is unproven and without Mauchly to tell his side, we felt that exploration of this part of computer history would only lead to the dead end of inconclusiveness.

We understand and appreciate the controversy regarding Atanasoff, but feel that our decision was correct. In the words of Sir Francis Darwin (in 1914): "In science, the credit goes to the man who convinces the world, not to whom the idea first occurs.

Producers, "The Machine That Changed the World"

[From dave marvit, wgbh@media.mit.edu]

## M The makers of the PBS series respond (Tompsett, <u>RISKS-13.37</u>)

WGBH-TV (Information Age) <wgbh@MEDIA-LAB.MEDIA.MIT.EDU> Thu, 9 Apr 92 18:38:05 EDT

We saw the posting by Brian Tompsett <br/>
bct@cs.hull.ac.uk> who asks ...

> Are we being manipulated by global telecasting> on an Orwellian scale? Who can tell? Not easy is it.

I can assure readers of RISKS that there is nothing Orwellian in the multi-versioning of the series. Jon Palfreman (executive producer) responds:

BBC programs are about 7 minutes shorter and that is the main difference. There are small differences of emphasis to reflect the interests and knowledge of the different audiences. For example, where there is a British figure who is well known he is mentioned (i.e. Sir Clive Sinclair

### ✓ Computer Users Foil Virus [Augments Slade, <u>RISKS-13.27</u>, for archives]

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 10 Apr 92 10:07:37 PDT

By Don Clark, c.1992, San Francisco Chronicle, 7 March 1992

Michelangelo claimed relatively few victims Friday, leaving experts to debate whether news media over-hyped the computer virus or performed a useful service by warning the public to take precautions. The virus apparently destroyed data in a few thousand personal computers around the world, far short of expectations. Researchers had estimated that the destructive software program had spread to anywhere from 100,000 to 5 million computers out of about 80 million IBM-compatible machines worldwide.

Most large businesses and institutions heeded the headlines and used special software to inspect and clean their personal computers before Michelangelo's birthday March 6, when the virus was set to go off. But some individuals and small businesses did not and came to regret it.

One of them was Bill Permar, a Sausalito accountant who turned on his computer to find that Michelangelo had destroyed the contents of two large disk drives containing his clients' tax data and other records. Although he had backup copies of that data, he was still struggling with his computer late Friday. ``I thought it was a lot of media hype,'' Permar lamented.

Michelangelo, written by an unknown prankster last year, caught the public imagination for several reasons. The program is among the most destructive of the more than 1,000 viruses in existence; when activated, the virus writes random characters over data on a personal computer's hard disk, making recovery almost impossible without backup copies of files. The program spreads through the exchange of floppy disks.

The widespread publicity over the March 6 deadline led to a drawn-out countdown on television, radio and in newspapers.

Some computer professionals think Michelangelo did a good deed by making millions of people aware of the danger of viruses. The state of California, for example, spent most of this week checking its thousands of personal computers for Michelangelo. Only one infection of that virus was found, but the check turned up other viruses on numerous machines.

On the other hand, some said the coverage may have unduly caused public hysteria and could inspire other pranksters to develop destructive programs. "I'm sure there are a dozen kids right now saying, 'I bet I can top that," said Joseph Pujals, the state's information security manager.

Michelangelo's typical victims include New Salem Baptist Church in Kennesaw, Ga.; Vigil Printing, a small firm in Chicago; and Save the Whales, the Venice (Los Angeles County) nonprofit group. Save the Whales lost its membership list, correspondence and a newsletter that was about to be printed.

Patricia Hoffman, a Santa Clara virus expert, said she had confirmed reports of 125 small U.S. businesses affected. American Telephone & Telegraph Co. confirmed that Michelangelo hit four of its 250,000 computers nationwide.

Other countries were hit harder. Some 750 to 1,130 personal computers in

South Africa reportedly were plagued by Michelangelo because of the widespread use of a bootleg version of the operating system used on IBM and compatible machines. Forty-eight companies or institutions were hit in Australia, 25 in Hungary, 10 in China and eight in Japan, Hoffman said.

Many victims were loath to admit that they did not take action, a possible factor in the low number of Michelangelo victims reported. ``They were warned," said Martin Tibor, a San Rafael data-recovery expert. ``If they got hit, it will be arrogance or stupidity."

One Bay Area public school with up to 20 stricken computers called Tibor but would not let its name be used, he said.

Some experts hope that Michelangelo will hasten the development of modified operating software that make it harder for viruses to be created and transmitted. "Some folks are working on it," said Peter Neumann, principal scientist in the computer-security group at SRI International in Menlo Park. "We need something on the order of a Chernobyl before people will wake up."

There is little doubt that the virus hype was great advertising for companies that specialize in selling virus-detection software. Symantec Corp., based in Cupertino, said it gave away 250,000 copies of a free program tailored to get rid of Michelangelo.

Friday, Symantec was logging about 33 Michelangelo-related calls per hour, with about 5 percent of those people claiming that their data was destroyed.

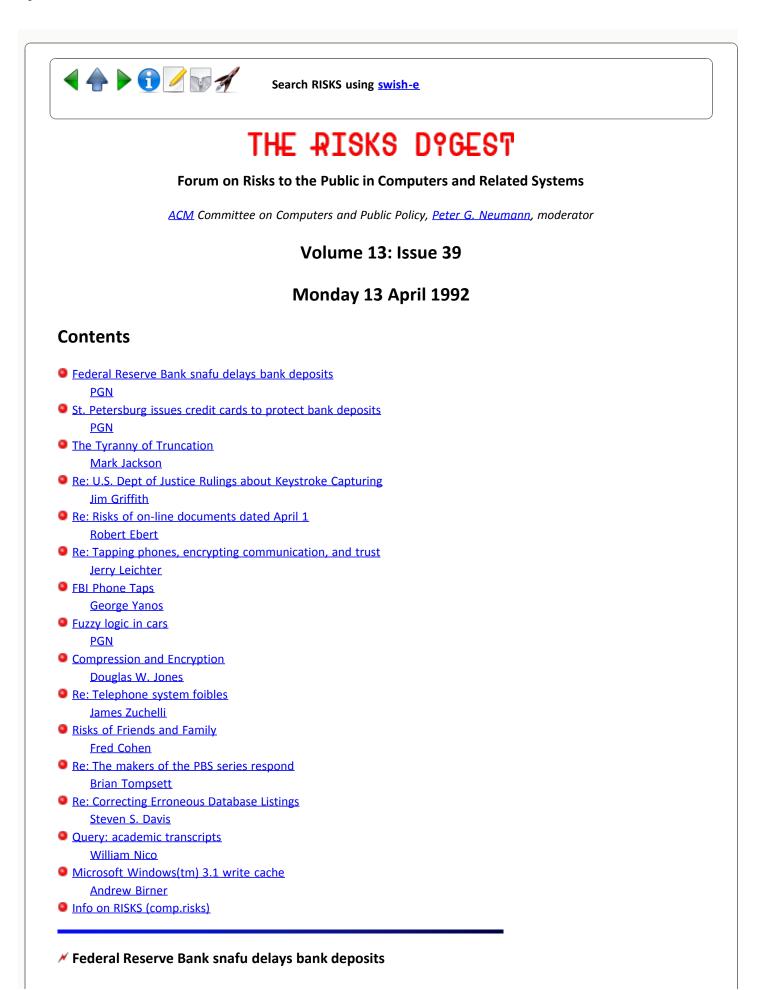
Another controversial topic is the effectiveness of anti-virus software. Some people claimed such programs did not work. ``There are a lot of really ticked off people,'' said John McAfee, a noted virus expert who runs a Santa Clara firm that sells anti-virus software. ``I think we're going to see some massive fallout in the anti-virus community.'' Manufacturers of anti-virus programs blamed the problem on the fact that customers failed to buy updated versions of the software that included protection against Michelangelo.

McAfee was criticized by some observers for suggesting that millions of computers had been infected. Friday, he estimated that 10,000 computers lost data worldwide.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Mon, 13 Apr 92 10:10:46 PDT

A computer failure at a Federal Reserve Bank data center in Los Angeles shut down computers for 12 hours on Friday, 10 Apr 1992 (payday) during the processing of debits and credits for about 90 banks, credit unions and S&Ls in California and Arizona. The unprocessed tapes were flown to San Francisco, but the data for at least 15 institutions were still not going to be processed until Monday. Some bounced checks were expected as a result of the missing payroll deposits. [Source: an article by Kenneth Howe, San Francisco Chronicle, 11 Apr 1992, p.B1]

#### X St. Petersburg issues credit cards to protect bank deposits

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 13 Apr 92 11:15:49 PDT

St. Petersburg, 13 April, TASS

By ITAR-TASS correspondent Lev Frolov: St. Petersburg has begun issuing credit cards to business people and bankers in an attempt to protect bank deposits from thefts. Unlike their western analogues, new plastic cards use holographic coding instead of traditional magnetic strips, which ensures 100 per cent guarantee from illegal withdrawals. The SPACARD system of credit cards developed by local specialists is part of the computer network "LEK TELECOM," which will include banks, insurance companies, exchanges and brokerage offices in Russia and other commonwealth states.

[ENSURES 100 PER CENT GUARANTEE, eh? And of course no one would ever misuse the computers...]

### The Tyranny of Truncation

<Mark\_Jackson.wbst147@xerox.com> Mon, 13 Apr 1992 04:38:16 PDT

According to the Rochester, NY, /Democrat & Chronicle/ of April 11, the Community College of the Finger Lakes is changing its name to Finger Lakes Community College. Although the changeover is expected to cost \$50,000, college officials say that greater expenses have arisen from confusion and omission of the two-year school from state and federal college registries.

According to college president Charles Mader, CCFL often gets short-changed by computerized listings that identify it as "Community College of the Finger."

Mark <MJackson.Wbst147@Xerox.COM>

**\*** Re: U.S. Dept of Justice Rulings about Keystroke Capturing

## <griffith@dweeb.fx.com> Thu, 09 Apr 92 11:08:06 -0700

Marc Horowitz (marc@MIT.EDU) questions the requirement of warning condo tenants about security TV cameras and the observation of someone committing an illegal act. It would probably be best if someone with more than a "Perry Mason" knowledge of law would answer this. But as I understand it, a person cannot have a audio- or videotape used against them unless the person either knew that the tape was being made at the time the crime was committed or the taping was done after a warrant was obtained based on probable cause. My guess is that prior knowledge followed by a deliberate illegal act or confession against interest constitutes consent. I don't fully understand this, because this doesn't seem to uniformly apply - there was a case recently where a man was a victim of gay-bashing on his front lawn, he captured it on videotape without the attacker knowing it, and the tape was used in court. I think the law says that without a warrant, one of the involved parties must have knowledge, with law enforcement agencies never being considered an "involved party".

Anyways, applying this to the issue at hand, a person electronically monitoring a login session in an automated manner would be treated the same way - without prior knowledge of the monitoring or a warrant, the evidence couldn't be used. If a user was on at the same time, issuing commands and determining from the result that something illegal was happening, then that user could act as a witness. But if a user sets up automated monitoring, then there are grounds for contesting it as illegal search and seizure.

Jim Griffith griffith@dweeb.fx.com

## Ke: Risks of on-line documents dated April 1 (Tarabar, <u>RISKS-13.37</u>)

<Robert\_Ebert.OsBU\_North@xerox.com> Wed, 8 Apr 1992 17:51:30 PDT

dtarabar@hstbme.mit.edu (David Tarabar) writes: >Not getting an April Fools joke might be more of a risk in on-line documents >because often they are not read until some time after the first of April.

I actually did read the TidBITS article on the 1st... call me slow, call me gullible.

In way of clarification, the two "inclusions" I sent from the #114 TidBITS were things purported to be the "truth", the \*rest\* of the article was the joke. Strangely, when I knew it was a joke and went back to look at it, I would have rated the IBM distribution article as "most likely to be false." What's next? Blue suits in airports singing, dancing, and giving away OS/2 in exchange for a "small donation"?

The joke articles consisted of:

Microsoft & NeXT?: An article about MicroSoft products for NeXT machines, and the pros and cons of such an arrangement. NeXT gets credibility as a business machine, MS gets stuff from the NeXT environment. Digs against Windows technology, NeXT popularity, and even ACE productivity. (All of which are, IMHO, deserved.)

#### Future Finder:

A long article about a new Finder replacement by Bruce Tognazzini. Lots of whizzy features, a DiskBox icon for unmounted floppies, groups of files called "collections", a super folder which launches everything inside when you doubleclick it, improved balloon help, and additionally fixing everything that's wrong with the Finder today. I don't care if it's a joke, I want it. I'll even take it in little pieces, via extensions.

#### New Life for Old Macs:

Okay, this is really the most obvious joke. Take your toaster Macs, swap out the motherboard, and put in a IIfx-like machine and maybe even a color LCD display with some weird backback BUS extensions. Nifty and impossible stuff here, but I was skimming at this point.

--Bob (bebert.osbu\_north@xerox.com)

## Tapping phones, encrypting communication, and trust

Jerry Leichter <leichter@lrw.com> Fri, 10 Apr 92 23:52:43 EDT

I'm disturbed by the tenor of the entire debate about phone tapping, privacy, and such. The general approach seems to be based on the idea that government is not to be trusted, ever, with anything. Nothing government says is to be believed.

Let's take the FBI "phone tapping" proposal. Everyone is absolutely sure that no technical changes are needed to tap any phone. The little the FBI has said contains no detailed information, so it's hard to tell exactly what they have in mind. But I submit that there is a clear instance today in which it would be difficult to insert an authorized tap. Suppose a company has a PBX, and the FBI has a court order to tap the line of the president of the company. Since the technicians running the PBX are employees of the company, the FBI can't work through them. Hence, they must go to the Telco side of the PBX. Unfortunately, calls coming out the PBX side need carry no identifying information about the calling extension - many PBX's are set up to return some fixed billing number for the whole company. So: It's easy to tap ALL calls coming out of the company - but how to you fulfill a court order allowing you to tap only those of the president? Do you really want the outcome to be that, in this case, the FBI is allowed to monitor ALL calls from the company?

Then there's the matter of "people shouldn't pay to have their own phones tapped." The lack of rationality in this argument is astonishing. It's like the argument: "Don't bill the taxpayers for the S&L bailout - let the government pay for it." If the FBI were to pay for the taps, where do you think its money would come from? Would you rather have the funding hidden in an anonymous budget paid for out of general revenues, or out there for all to

see? Object to the amount of money involved; object to this as a way around a "no new taxes" pledge; object to the very principle of the FBI EVER tapping phone conversations - but stop believing that government can give you something for nothing.

I submit that the right way to approach these issues is to first decide what authority we consider it desirable and proper to grant the FBI and other government agencies, then consider the effect of technological choices on their ability to exercise that authority. Here's an example: The much-argued proposed requirement that carriers have the capability to provide the government with the cleartext of encrypted messages. Suppose we decide that the current approach to tapping is correct: Upon presentation of appropriate evidence, the FBI is authorized to tap a line from some point on. Note that they cannot require the telephone company to record calls on the theory that they might later get a warrant to listen to them.

We can retain exactly this policy in a carrier-provided encryption system by requiring that the carrier, upon receipt of an appropriate court order, record and provide to the FBI all session keys created for the person being tapped. Unless a person was being tapped, the carrier would be under no obligation to record the keys; in fact, it should probably be obligated NOT to do so, just to avoid a temptation to implicitly expand the tapping authority.

It is quite true that people can use encryption devices outside of the carrier-provided system, thus rendering any aid the carrier can provide to the FBI useless. But there's nothing new here - that can be done today.

Any decisions about security and privacy must start with one fundamental decision: Whether we wish to provide privacy and security THROUGH LAW, or whether we wish an absolute security and privacy INDEPENDENT OF LAW. The working bias I see in virtually all submissions on these subjects is toward the latter approach. I would urge those who take this approach to examine their assumptions. Do they, for example, take the same approach to other kinds of protection provided by the government? Do they believe, for example, that we should banish policy departments and arm ourselves for our own protection against criminals, since some police have been shown to be corrupt?

-- Jerry

### FBI Phone Taps

George Yanos <U08208@UICVM.UIC.EDU> Sat, 11 Apr 92 08:50:55 CDT

"Disappointment" might be a better word, but in deference to the forum I'll ask: Which is the bigger risk, that nobody with the FBI is reading this, or that some of them are but that they refuse to join the discussion?

## 🗡 fuzzy logic

"Peter G. Neumann" <neumann@csl.sri.com> Sat, 11 Apr 92 12:10:50 PDT

Fuzzy-Mitsubishi: Mitsubishi motors to use fuzzy logic to make cars safer (Tokyo, 9 april 1992, kyodo)

Mitsubishi Motors Corp. said Thursday it has developed a new automobile safety feature that incorporates fuzzy logic chips to help reduce driver error and fatigue. Company officials said the system, called the Intelligent and Innovative Vehicle Electronic Control System (INVECS), uses fuzzy logic to control automatic transmissions, four-wheel drive and four-wheel steering systems, traction control systems, and electronically controlled suspension systems.

Fuzzy logic is a mathematical technique which, like human logic, deals with imprecise data that could lead to many solutions rather than one.

The new transmission system automatically downshifts gears to improve braking when the car is going downhill or when moving uphill shifts to a higher gear to eliminate sluggishness, the officials said. Currently, such shifting decisions must be made by the driver. Traction control systems will adjust engine power to handle flat, uphill, and downhill roads, while four-wheel drive controls vary the torque ratio between front and rear wheels to match driving conditions. The new four-wheel steering system moves the rear wheels in the opposite direction of the front wheels to enhance low-speed steering maneuvers. The new suspension system, which involves a sensor fitted to the front of the car body, improves riding comfort by adjusting the car to height differences in the road and lateral movement in the suspension system.

The officials said Mitsubishi plans to introduce the new safety system in a future car model.

## Compression and Encryption

Douglas W. Jones <jones@pyrite.cs.uiowa.edu> 12 Apr 92 21:32:43 GMT

> Could use of "non-standard" or uncommon compression techniques to > facilitate high-speed data transmission also be undesirable for the NSA/FBI?

In my CACM article "Application of Splay Trees to Data Compression," CACM 31, 8 (Aug. 1988) 996-1007, I pointed out that many compression algorithms have cryptographic applications. Adaptive model based compression algorithms start from an initial model state that converges as the data stream presented. The initial state of the model can be used as a key, and I proposed a trivial way to do this by throwing the key string at the model used in the compression and expansion programs prior to using those models to compress or expand data.

Here's the cryptographic algorithm, spelled out in painful detail:

Encrypt: Decrypt: Initialize-model Initialize-model for each ch in key loop for each ch in key loop update-model(ch) update-model(ch) end loop end loop looploopget(ch)uncompress-and-receive(ch)compress-and-send(ch)update-model(ch)update-model(ch)put(ch)end loop when ch=eofend loop when ch=eof

The above cryptographic algorithm works with my splay-tree-based codes, it works with Whitten Neal and Cleary's arithmetic codes, and it can even be fixed to work with such non-model-based adaptive compression schemes as LZW. Of course, some compression algorithms will make better encryption schemes than others, but I am aware of only a small amount of research on this.

It is worth noting that although most compression algorithms can be trivially modified to make them serve cryptographic purposes, I know of no attempt by the US government to limit the export of such code.

Doug Jones jones@cs.uiowa.edu

## Telephone system foibles (<u>RISKS-13.38</u>)

Tri-Valley Macintosh Users Group,UG <TMUG@applelink.apple.com> 12 Apr 92 11:52 GMT

I recently had two experiences with the telephone systems that leave me wondering if anyone knows what they are doing. I tried to make a call from a pay phone outside a restaurant in Sunnyvale, CA, using my calling card. The call wouldn't go through. The operator (from an alternative phone service) said that their computer showed I was trying to make a call from a correctional institution. I guess to avoid toll fraud, prisoners aren't allowed to make calling card calls.

In my next phone bill, (from an alternative phone service) there was a billing on my calling card for two calls made from Ada Mich. I've never been there and so had the charges deleted and changed my pin number. However after looking at the numbers listed, I found one was to a friend in San Jose. I now believe that the alternative phone service's computers somehow read some local calls as being made from Ada Mich.

What I'd like to know is how I can get all my calls misread so my phone bill will be cut in half?

However, even though this seems amusing, it makes one wonder just how inaccurate the alternative systems are. If they make these screwups, how many more do they make that are not detected? James Zuchelli

### Risks of Friends and Family

fc <FBCohen@DOCKMASTER.NCSC.MIL> Sun, 12 Apr 92 18:42 EDT

AT+T finally caught on, but they really didn't make the point very well.

The "friends and family" database being built by that other phone company will no doubt be sold so that when collecting a bill I will be ab;le to dial in and find your relatives and friends - in case you skip town. When I market something to you successfully, I will be able to claim your name when marketing to your friends and family. You can think of a lot of other examples of how this database might be abused.

It is somehow deeply offensive to me to be solicited to give the names of my friends and family in order to save money. I almost feel as if I am selling them out - literally! Tell me what birth control you use, and I will give you 10 bucks. Tell me how you have sex with your wife and I will give you 20! But be careful - I may get you arrested for having illegal sex!

I have an idea - How about royalties on all data stored in databases. If you keep data on me, I want you to pay me a dime per 80 bytes of info. If you sell it to someone else, I want 20% of gross as royalties. If it is inaccurate, I want to sue for damages. This would of course be the best way to control databases. After all, why shouldn't I be able to sell you the right to keep info on me. This would also clarify the relationship - I own all information about me, and you have to pay me to use it. If you don't keep accurate info, you are responsible for it - financially! To make certain it's right, you have to get my approval for its use. No waivers permitted, and no including this stuff in other agreements. Otherwise it will all be put into the standard contracts and people will hardly know it exists - but even that would be better than the current situation.

## Ke: The makers of the PBS series respond (Tompsett, <u>RISKS-13.37</u>)

Brian Tompsett <bct@cs.hull.ac.uk> Mon, 13 Apr 92 14:18:09 GMT

In RISKS-13.38 Dave Marvit (WGBH Associate Producer) writes that there is nothing Orwellian in the multi-versioning of TV programmes, and "The machine that changed the world/The dream machine" in particular. Contrariwise, I feel that there is some element of "Newspeak" involved in the programmes to (I quote) "reflect the interests and knowledge of the different audiences". When, for example, I see documented in programmes such as this "locals" such as Clive Sinclair and Joe Lyons Tea Shops I begin to wonder whether items about Bletchley Park Collossus, Manchester MADM, Cambridge EDSAC and other UK contributions to history are also there "to reflect the interests and knowledge of the different audiences". I can extend this analogy to imagine that the WGBH transmission reflects local Massachusetts "interest and knowledge" and is in some minor way different from the West coast and Central US transmissions for the same reasons. These programs can then be shown to local undergrads and every graduate will believe that "their" alma mater made \*the\* contribution to world development, because they saw it on TV. If this is not the Orwellian view of history then its pretty damn close.

We are drifting away from computer risks here, so let me attempt to bring the discussion back on track. If I applied my paranoid imagination to the Risks mailing list itself I can easily ask the same question. How do we know that the

items we receive in the UK on Risks are the same that arrive in the US? We don't, and in fact they are not the same. There are local UK postings to Risks readers that do not go to the US list. I can imagine for you an implementation where Risks articles from the US are put through a "jive" filter before going to the UK readership and vice-versa all UK contributions to the US list go through a "biffa" filter. This would have the effect of making each country think the other one was filled with yokels with a expletive filled vocabulary. Luckily for us, Risks is also published in paper form which helps to authenticate many of the contributions.

For those of you who are interested in these things, there is a US court case over the changing of TV programmes to "reflect the interests and knowledge of the different audiences". It involves the first US airing of "Monty Pythons Flying Circus" by a US network. The networks made "minor" changes to some sketches (removing some expletives) for a US audience. The python team sued and won, on the grounds that the changes substantially damaged their reputation. PBS, as the US readers now know, eventually broadcast Python in its unexpurgated form (BBC logos and all). Thanks should go to PBS for rendering this public service.

I hope readers don't think I'm trivialising the issue, or unnecessarily attacking reputable programme makers. On the contrary I think these issues are ones we should be aware of. We should "question" the media, and ensure that makers of exemplary documentary programmes such as "Nova/Horizon" do not cross that fine line between truth and ratings or history and Newspeak. When in the US I showed my support of WGBH at pledge time.

Brian Tompsett, Computer Science, University of Hull, UK.

### Ke: Correcting Erroneous Database Listings (Davis, <u>RISKS-13.36</u>)

Steven S. Davis <paa1338@dpsc.dla.mil> Mon Apr 13 13:04:55 1992

In <u>Risks 13.37</u>, Fred Gilham, responded to a proposal (in <u>Risks 13.36</u>) that an authoritative central database would provide protection against the spread of inaccurate data through different databases.

>... I think promulgation of inaccurate information should be legally >treated as a form of libel, ...

> -Fred Gilham gilham@csl.sri.com

That libel laws should be revised to take in to account libel by false inputs into databases is undeniably true. The problem with sole reliance on such laws to protect people against false information is threefold. It requires the wronged person to file suit each time the false data is promulgated, it does not set in place anything to stop further promulgations ( clearly, it's better to prevent damages than to collect them ), and it does not provide any protection to the operators of databases. Though my proposal emphasized the protection of people from the information in databases, I do not think it is in the public interest to impede the dissemination of correct data, which I fear successful libel prosecutions would, if they resulted in punitive damages sufficient to be a deterrent. The central database, once a correction were placed in it, would reduce further spread of the false data while greatly simplifying any actions for promulgating false data that still became necessary. It would also clarify the responsibility of the owners of databases to check for false information while providing a way of doing so. The database operator who has diligently checked the data received ( this would include checking the central database, but would not exclude other reasonable means of checking for errors ) should not be subject to the punitive damages that a more careless operator would richly deserve.

Steven S. Davis (ssdavis@dpsc.dla.mil)

### ✓ Query: academic transcripts

William Nico <nico@pyr.csuhayward.edu> Mon, 13 Apr 92 00:01:45 -0700

I have just learned from (senior and middle level) administrators at our campus, Cal. State U., Hayward, that serious consideration is being given to electronic exchange of academic transcripts between universities (actually between all levels of colleges, from community colleges on up). Our campus is apparently examining vendor information on such products, and I am told that San Jose State is actually involved in a pilot project (? alpha test ?) on this.

I have been able to get virtually no technical information from the administrators involved, except that discussion of such a process has been going on for some time among university admissions officers nation-wide and that there is even a recent (or proposed) ANSI standard (in X12?) on the matter. I am also told, naturally, that there are real products out there under development to implement such interchange.

The system seems fraught with risks to me, especially since universities form a much more heterogeneous (even anarchistic) community than, say, the banking community. My fragmentary information also indicates that there have been made (or are being made) some possibly strange design decisions. For example, it is reported that the products -- or the standard -- only allow 3 digits for a "course number" field; since our campus has traditionally used 4 digit course number, this would require renumbering the whole campus in order to participate is such a system.

Perhaps my main question is what sort of authentication/integrity mechanisms are to be used in such a system. the proposed new DSS? something DES based? something ad hoc? Will it require universities to purchase special hardware, or will it be software-based?

I think this issue may be of interest to a number of RISKS readers and that some of those readers may have good information to provide about what is being developed for transcript interchange. I, for one, would be very interested in hearing more on this topic.

-- Bill Nico W.R. Nico Mathematics and Computer Science California State University, Hayward Hayward, CA 94542-3092 e-mail: nico@csuhayward.edu

PS. --Moderator: This ran longer that I thought it would when I started. Feel free to edit it appropriately if you decide to use it to raise the issue. (Clearly, as moderator, you don't need my permission to edit, or delete, but it seemed like a nice thing to say.)

## Microsoft Windows(tm) 3.1 write cache

Andrew Birner <scsabir@tvgurus.hdtv.zenithe.com> Mon, 13 Apr 92 14:27:29 CDT

Microsoft's new version of Windows includes an "enhanced" version of the SmartDrv disk cache utility. The primary enhancement is the addition of a write-behind write cache. The RISKy part of this is that the default for the program is to enable the write cache on all hard drives; this is what the Setup utility suggests as the "preferred" configuration! Now, maybe I'm paranoid, but it seems to me that this is going to cause LOTS of problems for naive users. I'm especially worried because I don't believe that most casual users are going to bother reading through the documentation to find the little notice that says (on page 540):

CAUTION Check that SMARTDrive has completed all write-caching before you turn off your computer. To make sure this has happened, type SMARTDRV /C at the MS-DOS prompt. After all disk activity has stopped, you can safely turn off your computer.

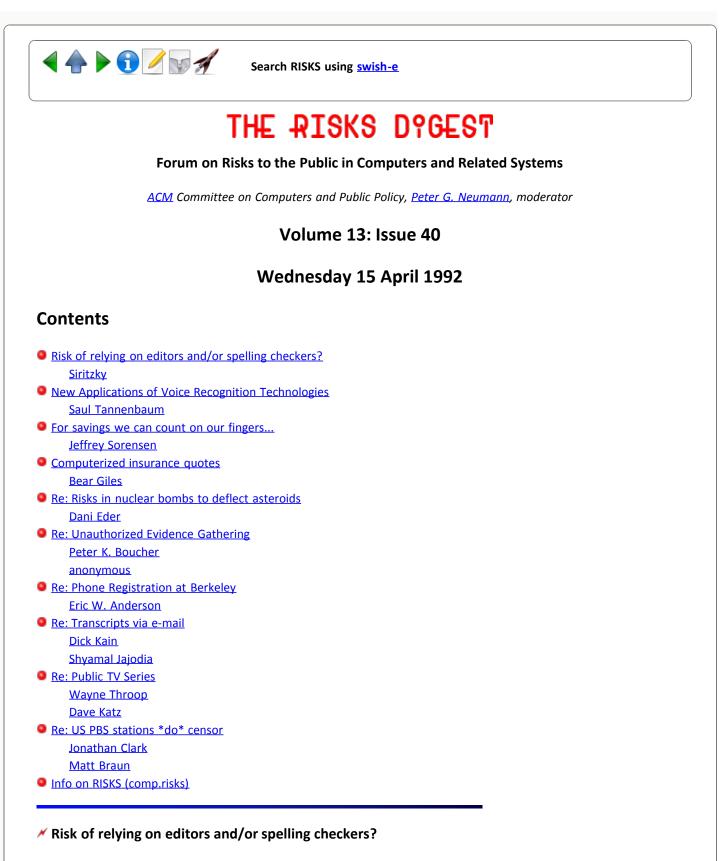
Personally, I think Microsoft has an incredible amount of confidence in the stability of 3.1, and in the diligence of the casual users; the decision to make this the default mode of operation was, in my view, ill advised.

- Andrew E. Birner, Zenith Electronics Corporation -



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<siritzky@apollo.hp.com> Tue, 14 Apr 92 14:06:39 -0400

The October 1991 issue of the New York University Law Review contained a note titled "Rethinking Adoption: A Federal Solution to the Problem of Permanency Planning for Children with Special Needs". On the front cover of the journal

and in the table of contents the note was listed with the word "abortion" used in place of "adoption". The correct title appeared on the note itself. Editors apparently only discovered the error when the received their advance copies, although it was also pointed out to them in a letter from Supreme Court Justice Harry Blackmun -- one of the authors of Roe v. Wade. [From: The National Jurist, March 1992, page 4]

### New Applications of Voice Recognition Technologies

Saul Tannenbaum <SAUL\_SY@hnrc.tufts.edu> Thu, 9 Apr 1992 13:32 EST

One of our local NPR (WBUR) stations had, in its morning news report, a story about a company that was developing a new twist in the application of voice recognition technologies. [I don't include the name of the company as I wasn't taking notes, and wouldn't want to needlessly slur the wrong company, or even the right one by my errors of recollection.]

Their goal is to develop a system that would be able to recognize not the words, but who the speaker is. The applications they envision would include control of parolees and those under house arrest, as well as the replacement of PINs. This is how they envision their system working:

- o The person who is to be monitored goes physically to the office doing the monitoring and records a set of words.
- o When the time comes for the person to be monitored to report in, they make a phone call to a computer system.
- o Caller-ID identifies who is supposed to be calling and their alleged physical location.
- o The system presents random challenge sentences that include some of the words used in step one. (One example: The purple television is exciting. "Television" and "exciting" would have been recorded.)
- o The system then isolates the pre-recorded words, compares the vocal characteristics and identifies the speaker.

Interesting concept. The company was quite proud that they had taken what has been a serious problem with voice recognition (voices are so different) and turned it into a technological advantage. It was asserted that a number of state correctional departments are interested in this as a replacement for the electronic bracelets that are now sometimes used to monitor house arrest and that have been discussed at length in RISKS.

The news report indicated that this system would be secure, as the comparison of vocal characteristics is not fooled by normal voice mimicry. It was also felt that, while parolees, for example, could be compelled to speak silly meaningless sentences into the phone, it might not be possible to do this generally so as to replace PINs.

This system seems so easy to defeat that I feel I must be missing something. When you go to record your words, bring your own micro-cassette recorder so that you've got an accurate list of the challenge words. Record and digitize them in your home personal computer. When time comes to report in, have your computer call their computer. Their challenge system seems quite structured (it already knows who you are supposed to be from the caller ID), so program your machine to wait for the challenge sentences. Recognize the right words from the list of the ones you've prerecorded, and synthesize a response based on replaying the challenge sentence, inserting your prerecorded words as necessary.

This technology is likely not within the reach of your average parolee, but should this system be used to authorize large financial transfers, the risk of fraud should be obvious.

Saul Tannenbaum, Manager, Scientific Computing STANNENB@HNRC.TUFTS.EDU USDA Human Nutrition Research Center on Aging at Tufts University

### For savings we can count on our fingers...

Jeffrey Sorensen <sorensen@spl.ecse.rpi.edu> Wed, 15 Apr 92 00:12:45 EDT

New York state's legislature is currently debating a proposal that would require Medicaid recipients to carry a photo ID and to be fingerprinted. While I think the proposal has a number of risks, for example amputees could experience \_another\_ cutback...

Seriously, this week's \_Legislative Gazette\_ (Apr 6 '92) amusingly demonstrates the risks of leaving politics to the politicians. Here are some of the insights:

Sen Hollings of NYC says between \$150 million and \$2 billion is wasted by fraudulent individuals. (Talk about ballpark figures)

Hollings: "It scares me to think of all the people that could have benefited from this money." (Well \_some\_ of those medicaid recipients are frightening. :-)

Republicans claim a similar system in LA saved the state \$5 million in the first year of operation.

With the electronic system, an individual places two fingers on a small flat screen. A computer then compares the fingerprints to those already on file.

Sen Farley of Schenectady said it didn't hurt, it wasn't messy and it took just a few seconds. (If you have nothing to hide, you have nothing to fear.)

The system costs LA \$2 million a year, but Farley says the cost doesn't compare with the savings (!?!). He estimates that New York could save \$16 million a year.

So there you have it, a system that will catch somewhere between 11% and 0.8% of the total fraud for the bargain price of \$2 million a year plus the setup fee. Shouldn't we have a better estimate if we are going to measure the

#### benefits of the system?

Further, I wonder how much saving can be attributed to the effectiveness of the system and how much is due to the perceived effectiveness of the system. There is this "scarecrow" effect that may not last in the long run. Perhaps some people will find work arounds. Perhaps New York should install a fake fingerprinting system with fake computers and fake databases at a lower cost and still get the same savings. Plus none of the civil liberties risks...

But no, this is not science, it is politics. ... fraudulent individuals wasting billions

Jeffrey Sorensen sorensen@ecse.rpi.edu

### ✓ Computerized insurance quotes

Bear Giles <bear@tigger.cs.colorado.edu> Wed, 15 Apr 1992 15:58:44 -0600

A while back I called a number of local insurance agents, getting quotes for my MR-2. During each call I made sure the agent knew 1) the MR-2 is an undiluted sports-car and 2) I have a clean driving record. (These are not mutually exclusive, though you will never get an insurance underwriter to admit it!)

Prudential Insurance quoted me a good rate (\$430, vs. my current \$620). I spent a lunch hour with the agent as he provided me an official quote from a worksheet program, signed a contract and paid the initial installment.

This worksheet program required the agent to specify insurance pool, type of vehicle, driver(s), mileage, etc. It even asked if my car was sheltered at home and/or work. This was definitely \_not\_ a program an agent cobbled together in his spare time.

Over a \_month\_ later I finally received my permanent insurance policy, including a demand for much more money. \$690 (total), to be precise. Prudential quickly agreed that all of the information I provided was correct -- it simply took them a month to notice that the agent had placed me in the incorrect insurance pool.

There was absolutely no indication in the quote worksheet program that new clients with MR-2s would not be accepted into the specified insurance pool -- it was 'assumed' the agent would know that. Unfortunately my agent only recently started working for Prudential and did not know MR-2s fell into this category.

At the current time, Prudential is insisting I pay the new amount despite being quoted a lower rate with accurate information. For now, I'm left paying more for insurance than I was with my previous insurer.

Meanwhile, I am filing a formal complaint with the state's Insurance Commission and Attorney General (was this bait-and-switch?), to say nothing of telling everyone within earshot about my experience. Prudential's legal expenses, in responding to these complaints, will almost certainly exceed the insurance premium.

The moral of the story: if you use a computer to determine contractual prices, if there are any 'gotchas' they should be explicitly noted by the software. I could accept Prudential changing the quoted rate if I mislead them about my driving history -- but not due to their failure to conduct business in accord with their own (internal) underwriting standards.

Bear Giles bear@fsl.noaa.gov

### Ke: Risks in nuclear bombs to deflect asteroids

Dani Eder <eder@hsvaic.boeing.com> 9 Apr 92 17:28:12 GMT

>change the orbit of asteroids heading towards the earth

About 25% of the risk is due to comets.

>4. NASA held two workshops to discuss this problem.

One of my co-workers, Dr. Brian Tillotson, attended one of the workshops, and I am working on a contract for the NASA guy who is responsible for this stuff (John Rather, NASA Asst. Director for Space Technology), although what I am working on is another subject (Laser power beaming).

>6. The last big collision of an asteroid with the earth was about 65 mill...

Don't forget about the Tunguska impact in 1908, and the impact that caused Meteor Crater about 25,000 years ago. We have lousy statistics on Earth-approaching asteroids in the 1-km size class (smaller than the supposed dinosaur killer, but still in the multi-gigaton of TNT energy class. There is expected to be on the order of 1000 of these, but we know of about 50 or so.

As for the risks/benefits:

In the past a large sudden explosion could happen and not much consequence beyond the immediate damage from the impact. Today, with early warning satellites in orbit, a meteorite impact could look suspiciously like a nuclear explosion. If it happened to be a sensitive military or political location that got hit, it could touch off a war. Even a kiloton impact (which would be much more common than a big one), could have this effect if it landed in the wrong place. So there is value in being able to detect incoming rocks and warn people beforehand, even if you can't deflect/destroy it.

Another side benefit, is getting good orbits for all these objects for later asteroid mining. The ones that come near the Earth are the ones that potentially are easiest to access for mining.

Long period comets are not mappable the way asteroids are, since they come from the depths of the Oort cloud, way beyond Pluto. They do make themselves bloody

obvious when they get to the inner solar system, so finding them is not the problem. Fortunately they have the consistency of a mudball, so blowing them away with a nuke is relatively easy. An iron-nickel asteroid, on the other hand, is a much harder problem to deal with. It is structurally harder and more difficult to vaporize. The issues of how to deal with these are more challenging. For now, the recommendations to upgrade the search for asteroids seems a fairly small cost to address a fairly small risk.

In a real emergency (comet discovered heading right for Earth, impact in 2 months), you can be sure that a nuke would get mounted on whatever rocket is handy in very short order and launched for an attempted interception. You can get a lot done if you work around the clock.

Dani Eder/Boeing/Advanced Civil Space/(205)464-2697(w)/232-7467(h)/ Rt.1, Box 188-2, Athens AL 35611/Member: Space Studies Institute

### ✓ Unauthorized Evidence Gathering (Griffith, <u>RISKS-13.39</u>)

"Peter K. Boucher" <boucher@csl.sri.com> Tue, 14 Apr 92 11:55:53 -0700

I don't know much about the laws in this area, but I have been following the Rodney King trial, where no-one involved knew they were being taped. Does the admission of this evidence set a new precedent?

If such evidence can be used against you, the obvious risk is that your privacy can be invaded on a massive scale in order to obtain the evidence. Of course they can invade your privacy already, they just can't use the results as evidence ;-) unless they've done their paperwork.

Peter K. Boucher boucher@csl.sri.com

### ✓ Use of taped evidence

<[anonymous]> Tue, 14 Apr 92 00:24:22 PDT

It would appear that permission, knowledge, or other prior information is not necessary for the use of taped materials in many cases, nor is it necessary for the person making the tape to be an "involved" party. A perfect example is playing itself out in the Los Angeles area right now, where the infamous "Rodney King" beating trial is drawing to a close. The most important evidence in the trial has been the videotape made by an uninvolved person living across the street. One would assume that the police involved did not have knowledge of the taping at the time of the event.

### Phone Registration at Berkeley

<EWANDERS@cmsa.Berkeley.EDU>

#### Wed, 15 Apr 92 15:52 PDT

The following article appeared in The Daily Californian, an independent newspaper distributed at UC Berkeley, April 14, 1992:

#### NO CLASSES FOR UNDECLARED IN TELEBEARS LIMBO

UC Berkeley sophomore Erica Oliver is caught in a registration Catch-22. Oliver says Tele-BEARS, the new registration-by-phone system heralded by students and administrators as a faster, more efficient way to get classes, won't let her enroll at all. The system will not place Oliver in the lower-division classes she needs to declare her major because she will be a junior next fall, but won't allow her to enroll in any upper division classes in her major because she hasn't declared it yet.

"It makes me feel very frustrated," Oliver said. "I just can't figure out why in the world I'm paying this university if I can't get any classes."

The phone-in system, initiated on campus last fall by a test group of 4,200 graduating seniors, guarantees students up to the maximum number of units their college allows. But the system doesn't guarantee students will be able to get into classes they need in order to declare or fulfill major requirements.

"Being a Junior, it's kind of late for not fulfilling the major requirements," Jorge Garza, acting associate registrar, said of Oliver's predicament. Garza said he recommends to students in situations similar to Oliver's to talk to an advisor about getting into the prerequisite classes.

But Margaret Distasi, director of student advising in Campbell Hall, said it may be difficult for undeclared students to get classes because major departments may reserve courses for declared students by prohibiting undeclared students from enrolling. Garza said students will simply have to declare as soon as possible in order to register for classes. "This is going to force students to process their paperwork (for declaring) faster," Garza said.

Garza said his office sent out more than 5,000 letters to students last fall offering a Tele-BEARS training session to inform students about how to prepare themselves for using the system. Only 39 students attended the session.

But on its second day of use by the whole campus, Garza said the registration process is going fairly smoothly. "Most students are getting classes even if they're not the ones they want because they haven't fulfilled certain requirements," Garza said. Tele-BEARS is scheduled to take 85 calls every 15 minutes during its operational hours, which Garza said would register the entire student population in 10 days.

#### [End of Quote]

This phone-activated registration system seems to avoid many of the risks that others have remarked on for similar systems at other universities. Each student is assigned a PIN unrelated to the student ID number. Each student has several possible time periods in which to register spread over the 10 day period. We won't know until it is through how many students will miss their time slots or otherwise fail to register properly, but the written information seems pretty clear and complete.

#### What are the RISKS here?

For one thing, they thought they had done a large-scale test of the system by having over 4000 students use it last semester. The flaw was that by limiting the test group to graduating seniors, they didn't test any number of complications that may only occur for undeclared students, freshmen, transfers, part-time students, those changing majors, etc. Repeating a simple test many times is not the same thing as showing that a procedure is flexible enough to handle the full spectrum of real-world inputs. They might have done a much better test by having 400 students from a range of departments and classes use the system rather than 4000 all from one class. (Of course, selecting students for the test at random might have been even better; by deliberately choosing some from every major, they might well have forgotten to test undeclared students.)

The second risk is less obvious. At the same time they replaced mail-in registration with the phone-in system, they changed the algorithm by which they assigned classes. Like many universities, Berkeley has difficulty offering enough sections of certain classes to satisfy demand. In the past, little checking was done to see whether a student was eligible to take a requested class. Now, many departments can limit registration in certain courses to students who have declared a major in that department. Apparently, they also now limit the ability of 3rd-year students to take lower division classed as well. Here the new method of ACCESSING the registration system is being blamed for a problem that could just as easily have arisen in the old one.

A third risk is best exemplified by the final quote from Garza. He appears to have changed the definition of successful registration from "getting the classes you want or need," to "getting any classes at all." It is hard to tell whether this is a case of retroactively changing the goals of a project to match the accomplishments, or whether this is just the way registrar's office droids see the problem of registration.

Eric W. Anderson, Chemical Engineering Dept., University of California Berkeley CA 94720 ewanders@garnet.berkeley.edu ewanders@CMSA.berkeley.edu

### // Transcripts via e-mail

R.Y. Kain <kain@ee.umn.edu> Wed, 15 Apr 92 11:53:55 -0500

I don't understand what the objective of such transfers would be, since most schools require authenticated paper copies of such documents before acting on them in any serious manner (such as admitting a student). The risks associated with restricting access to those authorized (not only to see any transcripts, but also to see specific transcripts - of designated individuals) seem quite high.

On another aspect - the course numbering system - let me relate our experience at the University of Minnesota with computerized academic record keeping. Such

records were kept by hand (pen and ink!) for longer than any one of us would believe. Then about 15-20 years ago they decided to install a computer to do the job. Before the change we had courses with identifiers that contained both letters and numbers, and some with one but not the other. For example, noncredit courses just had letters ("Math T" was remedial trig). And sequence courses had the same number with letter appendages (EE 30A, 30B, 30C). But then someone announced that the computer could only handle four-digit course numbers and we went through a long transition. This entailed conversion booklets working in both directions, and confusion among faculty who were used to advising the students based on the old numbers. After about three years it wore off. In EE we did obtain an advantage from the conversion - I suggested that we renumber so that the course number also indicated the sub-area within EE (thus computer related courses have numbers x350-x399 or x850-899, where x=3, 5, or 8). Why the x restriction? Well, nobody on campus is allowed to use numbers starting with 2, 4, 6, 7, or 9. And 0 and 1 correspond to no credit and lower division material, which doesn't include computers. (A long digression, but perhaps interesting to others... I think that the difficulty of conversion, etc. makes any "standard" that doesn't encompass ALL course numbering systems worthless. BUT that assumes that the access control and authentication issues are also satisfactorily resolved!)

Richard Y. Kain, EE Dept., University of Minnesota Mpls, MN 55455, 612-625-3537

### Ke: Academic Transcripts (Nico, <u>RISKS-13.39</u>)

Shyamal Jajodia <SHYAM@mitvmc.mit.edu> Wed, 15 Apr 92 17:04:10 EDT

Yes, it is true. The American Association of Collegiate Registrars and Admissions Officers (AACRAO) has a committee on SPEEDE (nifty eh!) for developing a national standard format for exchanging student transcripts over networks.

I agree with Bill Nico that the undertaking is fraught with risks but so is a trip to outer space. The important question is as Nico asks later what controls are being built in? I hope Bill is aware that grades can be obtained in several institutions over the phone even today.

The controls are no small matter because under the Family Education Rights Privacy Act (FERPA - Buckley Amendment) Universities must obtain written consent of the student before disclosing private records such as transcripts. I have seen this rule applied even when the person requesting the records is a parent of the student concerned.

I am also sure that a RISKS spotlight on this subject will help improve the controls in the system.

### **X** Re: Public TV Series

Wayne Throop <sheol!throopw@dg-rtp.dg.com>

13 Apr 92 22:01:02 GMT

<> [...] PBS will present "The Machine that Changed the World,"[...] <> Perhaps it is risky not to see how our <> industry is being popularized for the mass media.

Very true, I think. For example, in the very first program, I was interested to find out that Turing had established that anything a human can do, a computer can do.

Of course, on the other hand, a PBS series a year or two ago included the interesting fact that Searle had established that computers could never have true understanding.

> Their coverage of the historical material was the most accurate and
> even handed I have ever seen. Their coverage of risks issues is also
> exemplary. I could seriously use them in undergraduate teaching and did
> not regard them in any way as "technopulp" for the masses.

Hmmmm. I've only seen the first one so far, but it really seemed to fall prey to the common risk of many popularizations and simplifications of "scientific" results. A few other examples of the kind of thing I'm thinking of from physics: quantum theory "proves" that Zen Buddhism or Taoism or whatever-"eastern"-ism is correct after all, chaos theory is the explanation of QM effects, the uncertainty principle arises because observers affect the observed.

The problem is that in simplifying and dramatizing and analogizing ideas for presentation to "the public", much of the actual information is squeezed out, and incorrect factoids creep in as replacement. It isn't at all apparent what can be done about it, but it seems to me to be both commonplace and quite RISKy.

Mind you, I don't disagree that the series is "historically accurate", and I have no problem recommending it, if you watch it with a large grain of salt to hand. But it seems to me to be too quick to oversimplify complicated issues (such as the Turing bit above, and the reason binary encodings were eventually settled on, and many more).

Wayne Throop ... !mcnc!dg-rtp!sheol!throopw

### 🗡 PBS Program

Dave Katz <dkatz@cisco.com> Tue, 14 Apr 92 15:10:13 -0700

A few things shot by in last night's presentation that struck me as surprisingly pseudo-techno (rather than thoroughly techno, as most of the content of the programs have been). The most amusing was in the discussion of "higher level languages," during which a FORTRAN program scrolled by. It looked like FORTRAN in form, but close inspection revealed lines of code like:

151=15+1

An interesting assertion, but I suspect that even FORTRAN 66 compilers would reject it (rather than causing the booster rocket to fly off course, etc...).

Somebody had to do a whole lot of typing to create the "program." T'would have been much easier to use a real FORTRAN source (but of course this would introduce other RISKs that have been oft-discussed in this forum).

## VS PBS stations \*do\* censor

Jonathan Clark <jhc@iscp.bellcore.com> Tue, 14 Apr 1992 13:35:35 -0400

In Risks 13:39, Brian Tompsett says:

PBS, as the US readers now know, eventually broadcast Python in its unexpurgated form (BBC logos and all). Thanks should go to PBS for rendering this public service.

Alas, PBS have (at least partially) stopped doing this. Last year's rerun of I, Claudius had previously broadcast scenes cut from it (this was hinted at, but not spelled out, in Alistair Cooke's introduction). WNET (my local big PBS station) claimed that they presented the program the way it was given to them by WGBH. Paradoxically, WGBH's retail offshoot (Signals), in its advert for the videotapes of the series, claims that ``this is the original, uncut, British production, including some scenes not shown in the PBS broadcast''.

I have noticed that the ``same'' programs shown on the BBC and on PBS often have cuts, usually relating to sex scenes, when they are broadcast in the US. I, too, showed my feelings about the issue at pledge time, by \*withholding\* support, and telling the stations exactly why I was doing so.

Jonathan Clark, jhc@iscp.bellcore.com

### Ke: The makers of the PBS series respond (Tompsett, <u>RISKS-13.39</u>)

"Matt Braun" <mbraun@urbana.mcd.mot.com> Wed, 15 Apr 92 12:59:11 CDT

> For those of you who are interested in these things, there is a US

> court case over the changing of TV programmes to "reflect the

> interests and knowledge of the different audiences". It involves the

> first US airing of "Monty Pythons Flying Circus" by a US network.

> The networks made "minor" changes to some sketches (removing some

> expletives) for a US audience.

Actually, this isn't quite true. ABC (the network in question) SAID that all they were going to do was remove expletives. In reality, they were editing three 30-minute shows down into one 68-minute show, allowing some 24 minutes for commercials (i.e. they removed almost 25% of the material.) They deleted sketches, rearranged the order of some of them, etc. ABC did not make minor edits--they performed major surgery. It's sort of like going under the knife for an ingrown toenail and emerging minus one leg.

> The python team sued and won, on the
 > grounds that the changes substantially damaged their reputation.
 > PBS, as the US readers now know, eventually broadcast Python in its
 > unexpurgated form (BBC logos and all).

Yes, well, the changes \*did\* substantially alter the content of the program, and make the group appear to be less funny than they were. (For reference, see the excellent book by Robert Hewison, "Monty Python: The Case Against", ISBN 0-413-48660-5.)

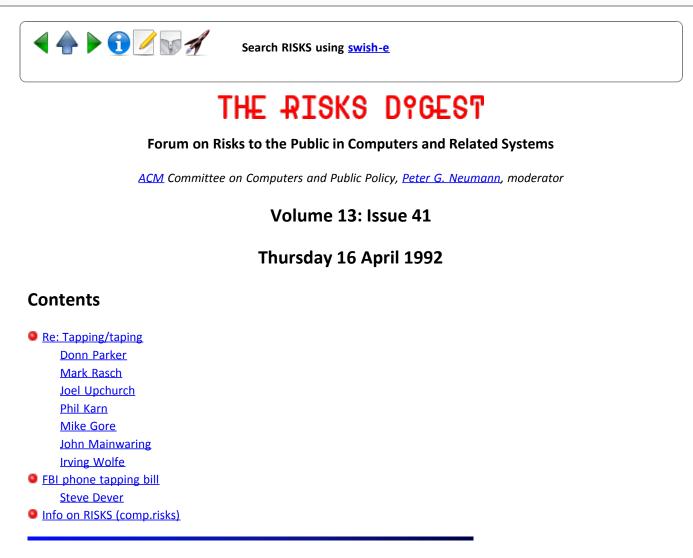
In the case of "The Machine That Changed The World", imagine trying to fit commercials into it, say at 8 minutes per half hour. (That seems to be close to the going rate here in the States.) Again, you'd have to lose about 1/4 of the program. I'd worry if they made edits because they don't want to offend "Mr. and Mrs. America". [... SLIGHTLY IMMODERATE BUT LIKELY EXAMPLES DELETED BY YOUR (IM)MODERATOR, TO STAVE OFF OBJECTIONS! PGN]

The Risk here? Um...the knives of the network gnomes? The Searing Scissors of the Censors?



Search RISKS using swish-e

Report problems with the web pages to the maintainer



## Intercept legislation

"Donn Parker" <donn\_parker@qm.sri.com> 16 Apr 1992 16:09:04 U

The Intercept law proposed by the FBI is in need of the full support of the cyberspace community but requires some additions that are disturbingly absent. The proposed amendment to the Communications act of 1934 is necessary to perpetuate an essential capability of law enforcement to protect the public from crime and particularly to protect the privacy of individuals whose personal information is communicated. However, it has serious shortcomings that must be corrected that I hope organizations such as EFF and CPSR can address that are needed to protect all the stakeholders from unauthorized use and misuse of the interception capability. Clearly, access and usage security controls are needed. In addition, recording of all intercept activity is needed for audit and evidential purposes. Finally, only the FCC rulemaking proceedings should be kept secret that would aid and abet unauthorized persons to abuse the capability to use the intercept capability for bad purposes; some detailed information about the auditing and safeguarding must not be revealed.

The providers and PBX operators probably require the interception capabilities anyway for maintenance and line quality testing. However, my suggested

additions would help ensure that interception for whatever reasons would not be misused, and abusers could more effectively be prosecuted. Donn B. Parker

#### Taping without consent

<Rasch@DOCKMASTER.NCSC.MIL> Thu, 16 Apr 92 16:59 EDT

There has been a lot of debate about whether a person can be videotaped (or audiotaped) without consent. The quick answer is it depends. Of course you can videotape people or objects if they are in the public view -- they have no legitimate expectations of privacy. Just look at The Star or other tabloids that routinely photograph people on the streets. There are limitations, however. There is a common law tort of interference with or invasion of privacy, as well as exploitation of a person's likeness for financial gain. (Suppose the "Coppertone" girl decided to sue). From a Fourth Amendment standpoint, a videotape in a public place is not an "unreasonable search or seizure."

Videotapes in PRIVATE places are another matter. Because they enable the government to see what otherwise cannot be seen, and therefore impart information to the government, they MAY constitute searches in Fourth Amendment terms. NOTE that the search (e.g., the videotaping) MUST entail some state action -- be performed at the behest of law enforcement. No state action -- no fourth amendment violation. (This does not prevent a private suit for interference with privacy, however). There is an exception recognized in Katz v. United States. That is, what Katz called the "invited ear" exception. You ALWAYS run the risk that the person you visit is videotaping you. (OR, in Katz, audiotaping you). This has led to the development of the law of one-party consent. IN GENERAL, one party to a conversation may consent to its being recorded. Exceptions exist in many jurisdictions for TELEPHONE conversations where the state law may require two party consent.

If the law always required two-party consent to video/audio recording, imagine the effect on -- for example -- television news. No more undercover recodings -- no more 60 Minutes. No more panoramic sweeps (consent from all the pedestrians??).

Finally, in the electronic environment things are even more screwy. Telephone calls are covered by privacy laws, FCC regulations, wiretap and surveillance laws, warrant requirements and the like. Electronic communications may also be covered by the Electronic Communications Privacy Act, the Privacy Protection Act, and (a la Steve Jackson) the First Amendment.

The turgidity continues.

### Ke: Tapping phones, encrypting communication, and trust

Joel Upchurch <upchrch!joel@peora.sdc.ccur.com> Tue, 14 Apr 92 04:52:49 EDT I would like to address what Jerry Leichter <leichter@lrw.com> said in <u>RISKS-13.39</u>. I agree with what he said about the ability of the FBI and other police authorities to tap into phone conversations being curtailed by the advances in technology. What I disagree with is that this is a bad thing. It seems to me that if tapping a phone conversation is difficult and expensive and the funding for such efforts comes out of the budget of the police agency involved, then it is far more likely that such tapping will be used with restraint, than if using it is cheap and easy.

If anything I'm worried that technology is going too far in the other direction. I suspect that the major cost of any phone tap isn't the cost of placing the tap and recording the conversations, but in paying people to listen to them. It isn't collecting data that is expensive, but analyzing it. With the advent of computer voice recognition in the next few years, it is quite possible that this cost will decrease drastically, maybe by an order of magnitude or more as the technology improves.

As the saying goes, government is a dangerous servant and a terrible master. A prudent citizen will try to ensure that powers of government are strictly curtailed and a close eye is kept to make sure these powers are neither abused or exceeded either through malice or an excess of zeal.

I keeping asking myself, how is the FBI proposal different from one that would require audio and video surveillance equipment be placed in every home at the expense of the home owner? Even if there were strict controls to make sure the equipment was never used without a court order, I doubt that most people would approve of it. What if the FBI required me to not seal my envelopes, since it would inhibit their ability to surreptitiously read my mail? It's not so much that idea that they want me to pay for it, it is the idea that want me to pay to give them capabilities that I'd be willing to pay for them NOT to have.

As for Mr. Leichter's police analogy, it is rather flawed. A better question to ask is should we forego the right of self-protection, because some criminals misuse the technology involved and always trust that the government will be able to protect us and will never oppress us? Some people think so, but I'm not one of them.

Joel Upchurch/Upchurch Computer Consulting/718 Galsworthy/Orlando, FL 32809 joel@peora.ccur.com {uiucuxc,hoptoad,petsd,ucf-cs}!peora!joel (407) 859-0982

### Ke: wire tapping (Leichter, <u>RISKS-13.39</u>)

Phil Karn <karn@chicago.Qualcomm.COM> Tue, 14 Apr 92 02:35:17 -0700

The debate over the FBI's proposal to ensure wiretappability of digital phone technologies largely misses the point. This is especially true for Jerry Leichter's recent comments.

I think it is reasonable to ask whether any proposed restrictive legislation will be effective in its intended purpose. If the answer is "no", then it is

entirely pointless to debate the merits of a bill's goals, no matter how desirable they may seem.

I submit that the FBI's measure will ultimately prove ineffective, for one very simple reason: user-provided end-to-end encryption. Like it or not, it is only a matter of time before most criminals routinely use it to thwart wiretaps. Encryption is uncontrollable because the encryption-specific parts of a system can be implemented entirely in software if necessary. It need only use cheap, readily available generic computer hardware that cannot be practically controlled in a modern industrial society.

The means to protect textual communications from wiretapping are already readily available. All it takes is a sufficiently motivated user. Someone, say, with good reason to fear an FBI wiretap. And before long the generic hardware necessary for secure voice communications will be just as cheap and widespread.

Eventually, the FBI's wiretap facilities will be effective only against those few remaining criminals too stupid to encrypt. And they could also be quite effective against those law-abiding companies and individuals who, instead of providing their own cryptographic privacy, blindly trust whatever "safeguards" (legal and/or technical) are supposedly in place to prevent their misuse. Quite frankly, after the Nixon years it's hard to have much faith in legal safeguards, and I know too much about telco technology to have much faith in technical safeguards.

Most readers of this list are highly computer literate, so these may seem like obvious statements. But they are apparently not so obvious to many in government policymaking positions. Our real problem is how to educate these people about the nature of cryptography, why it will be impossible for the FBI to maintain its precious "status quo", and to begin thinking about how they can \*realistically\* deal with the future instead of trying to force a return to the past.

We urgently need to get these people to understand the following:

1. The use of cryptography by criminals to thwart wiretaps is inevitable in anything remotely resembling a modern free society. You don't even want to contemplate living in a state with truly effective ways to prevent the private use of encryption. So we might as well promote, not restrict, the widespread use of encryption so that law-abiding persons can benefit from it as well.

2. As the utility of the wiretap decreases, law enforcement will have to rely other ways to collect evidence. Informers, for example, or testimony compelled under grants of immunity. Eventually the government might even have to consider abandoning its attempts to penalize certain types of behavior that consist largely or entirely of communications or the mere possession of information.

Unfortunately, our government's historical inability to accept the inevitable without a long, wasteful and futile fight does not give me much hope that we'll avoid one this time.

Phil

## FBI Phone Taps (Re: <u>RISKS-13.39</u>)

Mike Gore <magore@icr2.waterloo.edu> Tue, 14 Apr 92 11:58:18 -0400

I submit that the biggest risks in dealing with a system that allows single point phone tapping can be better addressed in questions far more basic then of trusting the good intentions of any agency itself. Rather we might first examine:

- 1) The number of lives and total value of all information to be entrusted to such a system.
- 2) The ability of such an agency to protect the proposed system from misuse by outside forces.
- 3) The social and monetary costs including the risks generated from proposed system vs that of the former system .

So even if one fully trusts the intentions of an agency we might not sleep better knowing that we have in effect put up a big sign saying to all would be criminals "in order to save you time we have placed all are eggs in this basket right here"...

Mike Gore, Technical Support, Institute for Computer Research 1-519-885-1211, x6205 uunet!watmath!watserv1!magore magore@watserv1.waterloo.edu or magore@watserv1.uwaterloo.ca

## Ke: Telephone system foibles - also cryptography

John (J.G.) Mainwaring <CRM312A@BNR.CA> 14 Apr 92 17:49:00 EDT

James Zuchelli seems surprised that he would have calls billed by Alternate Operator Services companies from places he's never never been. The practice is known as 'Splashing', and arises from the arrangements among smaller long distance carriers and operator services companies. His call was presumably handled by an operator company in Ada, Michigan who were unable to determine the true point of origin of the call. They would bill the call to a calling card as being from their location to the actual called number. Congress and the FCC do not seem to feel that this practice was one of the benefits intended to follow from the break up of the Bell System, and seem to have initiated proceedings to ensure that all calls will be billed based on the true point of origin.

The FBI/encryption/privacy debate has been interesting. Obviously the FBI will only be successful in interpreting data from wiretaps if they can manage to stay abreast of technology. The usual file archiving and compression schemes are meant to be easy to use, so any reasonbly aware user will recognize from file naming conventions what decompression techniques to use. They could become the basis for encryption schemes, but it seems reasonable to suppose that they would tend to have signatures that a knowledgeable spook could recognize fairly easily. In the same way, the FBI would have to keep abreast of technology and learn to use any widely used speech compression technology. ISDN makes end to end encryption of speech a little easier than it once was, since speech is readily available for manipulation in digital form at either end. However, it's possible to compress digital speech from the 64K bit/sec rate ISDN normally uses to rates as low as 2400 bit/sec with some loss of fidelity, and that would allow a digital stream to be encrypted and transmitted on a fairly ordinary analogue line. Any digital switch would allow the FBI to wiretap such a call, but it would take them a good deal of effort to make sense of it.

Ultimately it seems unlikely that laws against using encryption will deter people who are already breaking more serious laws. They will affect people with legitimate needs for privacy such as protection of trade secrets and financial information. Restrictions on American trade will clearly not apply abroad, and can only work to the disadvantage of American (free?) enterprise. The FBI may wish for simpler times, but in the long run it seems like they'll have to heat their buildings with Crays and learn to be as good at cryptography as the bad guys. After all, the first working electronic computer may have been Colossus, which was built to do cryptography.

### Ke: Tapping phones, encrypting communication, and trust

Irving\_Wolfe <irving@happy-man.com> Wed, 15 Apr 1992 16:17:27 GMT

>I'm disturbed . . . . The general approach seems to be based on>the idea that government is not to be trusted, ever, with anything.>Nothing government says is to be believed.

Many of us do feel that the history of government lies on issues large and small preclude believing what government tells us without substantial additional evidence. Sure, there are many good people in government, and many useful functions performed by it. But we really do differ from you in having enough concern for civil liberties to willingly, even enthusiastically accept some inefficiency and some additional crime in return for stronger guarantees of privacy and freedom for the great masses of people who are basically decent, including ourselves and our friends.

>Let's take the FBI "phone tapping" proposal.

Many of us, while tolerant of occasional phone-tapping under a difficult-to-get court order, might prefer no phone-tapping at all to tapping under easy-to-obtain court orders or widespread tapping of any sort.

>Do they believe ... that we should banish policy [sic] departments >and arm ourselves for our own protection against criminals ... ?

We might not advocate the abolition of police departments because they have not yet become that extremely corrupt. But for other reasons -- including the physical inability of even a large police force to provide protection at the level that could assure everyone's safety from assault, burglary, rape, and murder -- we certainly support possession of firearms by adult citizens, perhaps even required possession and required training. This threat of self-defense would produce a far greater reduction in violent crime than any law could.

The risks issue, as I see it: I'm happy to assume the (perceived small) risk that my neighbor will shoot me, in place of the (perceived much larger) risk that either a criminal will attack my family and friends while we are defenseless or that at some future time only a fully armed population could save itself from a would-be-totalitarian government (either home-grown or invading). It is no accident that the Soviet Union's first action after taking over Hungary, Czechoslovakia, and Poland was the seizure of privately owned firearms.

Irving\_Wolfe@Happy-Man.com Happy Man Corp. 206/463-9399 x101 4410 SW Pt. Robinson Rd., Vashon Island, WA 98070-7399 fax x108 [Commercial advertising deleted... PGN]

### FBI phone tapping bill

Steve Dever <Steve.Dever@eng.sun.com> Wed, 15 Apr 92 10:06:55 PDT

Attached is a copy of the FBI's proposed law which would prevent telephone companies and PBX operators from using equipment which would inhibit the government's ability to perform wiretaps. This was uploaded to the Well by Mike Godwin of the EFF.

Steve Dever

102nd Congress 2nd Session

Amendment No. Offered by M.

- 1. SEC. 1. FINDINGS AND PURPOSES
- 2. (a) The Congress finds:
- 3. (1) that telecommunications systems and networks are often
- 4 used in the furtherance of criminal activities including
- 5 organized crime, racketeering, extortion, kidnapping, espionage,
- 6 terrorism, and trafficking in illegal drugs; and
- 7 (2) that recent and continuing advances in
- 8 telecommunications technology, and the introduction of new
- 9 technologies and transmission modes by the telecommunications
- 10 industry, have made it increasingly difficult for government
- 11 agencies to implement lawful orders or authorizations to
- 12 intercept communications and thus threaten the ability of such
- 13 agencies effectively to enfore the laws and protect the national
- 14 security; and
- 15 (3) without the assistance and cooperation of providers of
- 16 electronic communication services and private branch exchange
- 17 operators, the introduction of new technologies and transmission
- 18 modes into telecommunications systems without consideration and
- 19 accommodation of the need of government agencies lawfully to
- 20 intercept communications, would impede the ability of such
- 21 agencies effectively to carry out their responsibilities.

- 1 The purpose of this Act are:
- 2 (1) to clarify the duty of providers of electronic
- 3 communication services and private branch exchange operators to
- 4 provide such assistance as necessary to ensure the ability of
- 5 government agencies to implement lawful orders or authorizations
- 6 to intercept communications; and
- 7 (2) to ensure that the Federal Communications Commission,
- 8 in the setting of standards affecting providers of electronic
- 9 communication services or private branch exchange operators, will
- 10 accommodate the need of government agencies lawfully to intercept
- 11 communications.
- 12 SEC. 2. Title II of the Communications Act of 1934 is amended
- 13 by adding at the end thereof the following new sections:
- 14 "Sec\_\_. GOVERNMENT REQUIREMENTS
- 15 "(a) The Federal Communications Commission shall,
- 16 within 120 days after enactment of this Act, issue such
- 17 regulations as are necessary to ensure that the government
- 18 can intercept communications when such interception is
- 19 otherwise lawfully authorized
- 20 "(b) The regulations issued by the commission shall:
- 21 "(1) establish standards and specifications for
- 22 telecommunications equipment and technology employed by
- 23 providers of electronic communication services or
- 24 private branch exchange operators as may be necessary
- to maintain the ability of the government to lawfully
- 26 intercept communication
- 1 "(2) require that any telecommunications
- 2 equipment or technology which impedes the ability of
- 3 the government to lawfully intercept communications and
- 4 and which has been introduced into a telecommunications
- 5 system by providers of electronic communication
- 6 services or private branch exchange operators shall not
- 7 expanded so as to further impede such utility until
- 8 that telecommunications equpment or technology is
- 9 brought into compliance with the requirements set forth
- 10 in regulations issued by the Commission;
- 11 "(3) require that modifications which are
- 12 necessary to be made to existing telecommunications
- 13 equipment or technology to eliminate impediments to the
- 14 ability of the government to lawfully intercept
- 15 communications shall be implemented by such providers
- 16 of electronic communication services and private branch
- 17 exchange operators within 180 days of issuance of such
- 18 regulations; and
- 19 "(4) prohibit the use by electronic communication
- 20 service providers and private branch exchange operators
- 21 of any telecommunications equipment or technology which
- 22 does not comply with the regulations issued under this
- 23 section after the 180th day following the issuance of
- 24 such regulations.
- 25 "(c) For the purposes of administering and enforcing

- 26 the provisions of this section and the regulations
- 1 prescribed hereunder, the Commission shall have the same
- 2 authority, power, and functions with respect to providers of
- 3 electronic communication services or private branch exchange
- 4 operators as the Commission has in administering and
- 5 enforcing the provisions of this title with respect to any
- 6 common carrier otherwise subject to Commission jurisdiction.
- 7 Any violation of this section by any provider of electronic
- 8 communication service or any private branch exchange
- 9 operator shall be subject to the same remedies, penalties,
- 10 and procedures as are applicable to a violation of this
- 11 chapter by a common carrier otherwise subject to Commission
- 12 jurisdiction, except as otherwise specified in subsection13 (d).
- 14 "(d) In addition to any enforcement authorities vested
- 15 in the Commission under this title, the Attorney General may
- 16 apply to the appropriate United States District Court for a
- 17 restraining order or injunction against any provider of
- 18 electronic communication service or private branch exchange
- 19 operator based upon a failure to comply with the provisions
- 20 of this section or regulations prescribed hereunder.
- 21 "(e) Any person who willfully violates any provision
- 22 of the regulations issued by the Commission pursuant to
- 23 subjection (a) of this section shall be subject to a civil
- 24 penalty of \$10,000 per day for each day in violation.
- 25 "(f) To the extent consistent with the setting or
- 26 implementation of just and reasonable rates, charges and
- 1 classifications, the Commission shall authorize the
- 2 compensation of any electronic communication service
- 3 providers or other entities whose rates or charges are
- 4 subject to its jurisdiction for the reasonable costs
- 5 associated with such modifications of existing
- 6 telecommunications equipment or technology, or with the
- 7 development or procurement, and the installation of such
- 8 telecommunications equipment or technology as is necessary
- 9 to carry out the purposes of this Act, through appropriate
- 10 adjustments to such rates and charges.
- 11 "(g) The Attorney General shall advise the Commission
- 12 within 30 days after the date of enactment of this Act, and
- 13 periodically thereafter, as necessary, of the specific needs
- 14 and performance requirements to ensure the continued ability
- 15 of the government to lawfully intercept communications
- 16 transmitted by or through the electronic communication
- 17 services and private branch exchanges introduced, operated,
- 18 sold or leased in the United States.
- 19 "(h) Notwithstanding section 552b of Title 5, United
- 20 States Code or any other provision of law, the Attorney
- 21 General or his designee may direct that any Commission
- 22 proceeding concerning regulations, standards or
- 23 registrations issued or to be issued under the authority of

- 24 this section shall be closed to the public.
- 25 "(i) Definitions -- As used in this section --
- 1 "(I) 'provider of electronic communication
- 2 service' or 'private branch exchange operator' means
- 3 any service which professes to users thereof the ability
- 4 to send or receive wire, oral or electronic
- 5 communications, as those terms are defined in
- 6 subsections 2510(1) and 2510(12) of Title 18, United
- 7 States Code;
- 8 "(2) 'communication' means any wire or electronic
- 9 communication, as defined in subsection 2510(1) and
- 10 2510 (12), of Title 18, United States Code;
- 11 "(3) 'impede' means to prevent, hinder or impair
- 12 the government's ability to intercept a communication
- 13 in the same form as transmitted;
- 14 "(4) 'intercept' shall have the same meaning
- I5 set forth in section 2510 (4) of Title 18, United States16 Code:
- 17 "(5) 'government' means the Government of the
- 18 United States and any agency or instrumentality
- 19 thereof, any state or political subdivision thereof,
- 20 and the District of Columbia, and Commonwealth of Puerto
- 21 Rico; and
- 22 "(6) 'telecommunications equipment or technology'
- 23 means any equipment or technology, used or to be used
- 24 by any providers of electronic communication services
- 25 or private branch exchange operators, which is for the
- 1 transmission or receipt of wire, oral or electronic
- 2 communications."
- 3 SEC 3. Section 510, Title V, P.L. 97-259 is amended deleting the
- 4 phrase "section 301 or 302a" and substituting the phrase "section
- 5 301, 302a, or \_\_\_\_\_.

DIGITAL TELEPHONY AMENDMENT (report language)

Significant changes are being made in the systems by which communications services are provided. Digital technologies, fiber optics, and other telecommunications transmission technologies are coming into widespread use. These changes in communications systems and technologies make it increasingly difficult for government agencies to implement lawful orders or authorizations to intercept communications in order to enfore the laws and protect the national security.

With the assistance of providers of electronic communication services, these technological advances need not impede the ability of government agencies to carry out their responsibilities. This bill would direct the Federal Communications Commission (FCC) to issue standards ensuring that communications

systems and service providers continue to accommodate lawful government communications intercepts. The regulations are not intended to cover federal government communications systems. Procedure already exist by which the Federal Bureau of Investigation amy obtain federal agency cooperation in implementing lawful orders or authorizations applicable to such systems. Further, there would be no obligation on the part of the service providers or any other party to ensure access to the plain text of encrypted or other encoded material, but rather only to the communication in whatever form it is transmitted. It is thus the intent and purpose of the bill only to maintain the government's current communications interception capability where properly ordered or authorized. No expansion of that authority is sought.

#### ANALYSIS

Subsection 2(a) and (b) would require the Federal Communications Commission (FCC) to issue any regulations deemed necessary to ensure that telecommunications equipment and technology used by providers of electronic communications services or private branch exchange operators will permit the government to intercept communications when such interception is lawfully authorized. The regulations would also require that equipment or technologies currently used by such providers or operators that impede this ability until brought into compliance with the regulations. Compliance with FCC regulations issued under this section would be required within 180 days of their issuance.

Subsection 2(c) provides that the Commission's authority to implement and enforce the provisions of this section are the same as those it has with respect to common carriers subject to its jurisdiction.

Subsection 2(d) would give the Attorney General the authority to request injunctive relief against non-complying service providers or private branch exchange operators.

Subsection 2(e) provides civil penalty authority for willful violations of the regulations of up to \$10,000 per day for each violation.

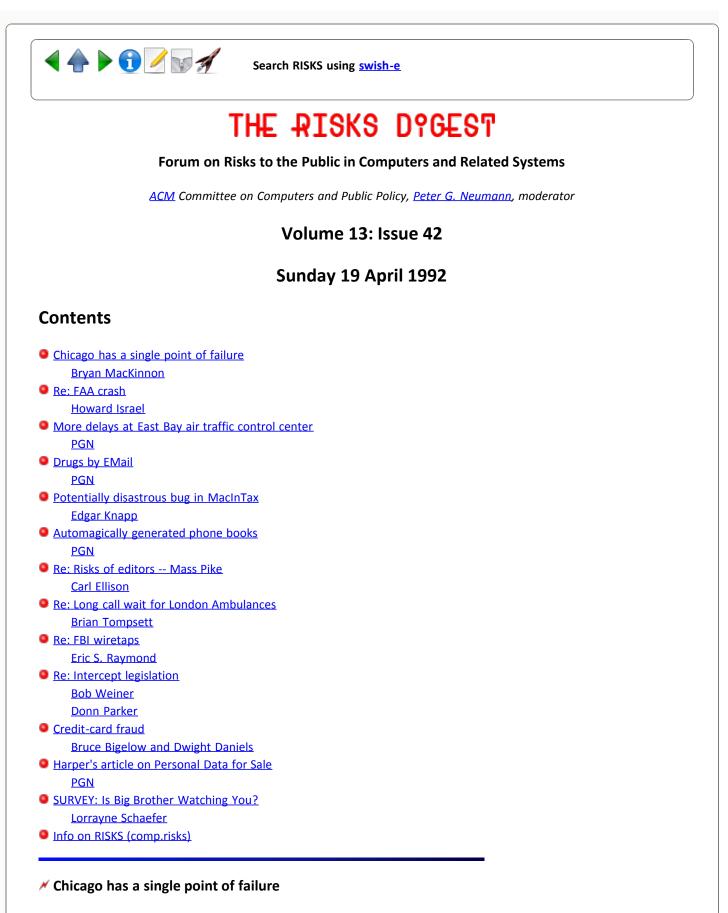
Subsection 2(f) would permit the FCC to provide rate relief to service providers subject to its rate-setting jurisdiction for the costs associated with modifying equipment or technologies to carry out the purposes of the bill.

Subsections 2(g), (h), and (i) require the Attorney General to advise the Commission regarding the specific needs and performance criteria required to maintain government intercept capabilities, require the FCC to ensure that the standards and specifications it promulgates may be implemented on a royaltyfree basis, and authorize the Attorney General to require that particular Commission rulemaking proceedings to implement the Act be closed to the public.

Subsection 2(j) provides definitions for key terms used in this section.



Report problems with the web pages to the maintainer



Bryan MacKinnon <mackinno@fndaut.fnal.gov> Thu, 16 Apr 1992 09:36:26 -0500 On April 13, 1992, Chicago experienced the closest thing to the "Chicago Fire" this century. It is not news to most people now that the forty to sixty miles of century old freight tunnels underneath the "Loop", or main downtown area, were flooded on that fateful day. It appears to be caused by a recently installed bridge piling that breached the tunnel where is passes under the Chicago River. When built, these tunnels were used for transporting coal, newsprint, and many other items on an electric railway.

The risks to computing were/are significant. Although no longer used to transport freight, they are now used as conduits for communication cables (fiber, etc) that connect together the city's main business district. Furthermore and more damaging, the tunnels connect the basements of numerous buildings which are now flooded. These flooded basements are home to telephone and electrical equipment, most of which were disabled for days. The loss so far to the city is easily over \$500M and expected to exceed \$1B.

But the main reason that I submit this message to risks is more to do with a classic design flaw of any complex system, in this case, a city: Chicago has a single point of failure.

Bryan MacKinnon, Fermi National Accelerator Lab Batavia, IL 60510 (within spectating distance of Chicago).

### Re: FAA crash (<u>RISKS-13.37</u>)

Howard Israel <hmi@neptune.att.com> Wed, 15 Apr 92 15:04 EDT

A software bug in a crucial FAA computer, one that programmers had identified and had planned to fix Friday, acted up Wednesday morning before they could get to it, shutting down the computer and disrupting Northern California air traffic for about 2 1/2 hours. A spokesman for the Federal Aviation Administration said a back-up computer system immediately kicked in and that while departing flights were held back at many airports, no planes in the air during the shutdown were ever endangered. [San Jose Mercury News, 9 Apr 1992]

---Howard Israel, AT&T Bell Labs, 201 386 4678

### More delays at East Bay air traffic control center

"Peter G. Neumann" <neumann@csl.sri.com> Sun, 19 Apr 92 13:06:58 PDT

The Oakland Air Route Traffic Control Center in Fremont CA had receivers for 12 of its 50 radio frequencies go dead on 17 April 1992. The partial outage lasted for about 1.5 hours and delayed 36 outgoing flights from San Francisco (up to 27 minutes), 7 from Oakland, and one from San Jose. The reason was undetermined. [Source: San Francisco Chronicle, 18 Apr 1992, p.A13]

## ✓ Drugs by EMail

"Peter G. Neumann" <neumann@csl.sri.com> Sun, 19 Apr 92 12:59:54 PDT

Two men have been arrested for selling cocaine via the Charles Schwab company EMail, where they had been employed in the back-room of the San Francisco office. The company has a vigilant policy against drugs in the workplace, although the National Institute of Drug Abuse estimates that 10 percent of the country's workforce regularly uses drugs while at work. [Source: San Francisco Chronicle, 18 Apr 1992, p.A13]

### Potentially disastrous bug in MacInTax

Edgar Knapp <knapp@cs.utexas.edu> 15 Apr 92 08:32:31 GMT

[Forwarded to RISKS by nick@dcs.edinburgh.ac.uk]

[NOTE from the moderator: I have no way to confirm this bug report but given the critical date and the fact that the IRS isn't going to care whose fault it was, and the standard software warranty doesn't promise anything to the purchaser anyway, I hope you will agree with me that approving this article is the right thing to do at this time. ---Werner ]

There is a recalculation bug in MacInTax which can lead to income not being reported. The problem occurs when opening a previously saved tax data file. MacInTax often and reproducibly fails to correctly incorporate certain types of income (1099-Misc, for instance). This can lead to IRS audits and penalties, since income reported on the return and income reported directly to the IRS don't match.

The work-around for the problem is to force a recalculation of the income entered into MacInTax, by unchecking and rechecking the Routing Information box of at least one of the affected 1099s in "FORM 1099: Miscellaneous Income Statement".

ChipSoft is aware of the bug, but prefers to call it an inadvertent inaccurate recalculation problem.

Also, even though this is not 100% reproducible, make sure you save you return before selecting "Open Notes..." from the Windows menu, or La Bomba may make tax time even more taxing.

Edgar (knapp@cs.utexas.edu)

### Automagically generated phone books

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 17 Apr 92 17:07:55 PDT

SRI just issued an errata sheet on the new telephone directory.

- \* The parking lot and road overlay on the building graphic was printed upside down, with North and South reversed. It sure looked strange.
- \* The Office of Corporate Compliance was erroneously listed as the Office of Corporate Complaints in the list of FREQUENTLY USED PHONE NUMBERS. Perhaps they know something I didn't. I didn't think the correct listing would be frequently used, although the erroneous one might.

### Ke: Risks of editors -- Mass Pike

<Carl\_Ellison@vos.stratus.com> Thu, 16 Apr 92 11:47 EDT

The Massachusetts Turnpike handed out a nicely printed flier the other day, advertizing their maintenance plans (and trying to get some PR, no doubt). This flier included the sentence "Since the initial turnpike was opened to traffic in 1957, billions of vehicles have traveled over the 135-mile road and its 260 brides [sic], and these facilities are showing the ravages of time and traffic."

This example is just cute -- but representative. In the inefficient old days, so many different humans were involved in the process ending with typesetting that typos like this almost never made it into print.

We have made editors, spelling checkers, grammar checkers (all of which allow that typo to happen). How are we going to get back the level of checking we had when it took 5 different people to get something printed?

[The opera The Bartered Bride is often cited in print as The Battered Bride. But don't forget that some typos are inserted rather intentionally by frustrated typesetters. I have one dandy that cannot be repeated here. PGN]

### Ke: Long call wait for London Ambulances (<u>RISKS-13.38</u>)

Brian Tompsett <bct@cs.hull.ac.uk> Thu, 16 Apr 92 11:12:13 GMT

From the BBC Radio 4 programme "Punters" broadcast this morning 16th April 92. An item was about the long time callers have to wait for the London Ambulance Service to answer the phone after an emergency call (999). The programme mentioned several cases where callers waited up to 15 minutes for the central Ambulance control room to answer the phone. During that time the BT (Phone Company) operators are handling the call. The operators tell of hearing people die on the other end of the phone while the ambulance station plays a recorded message "please hold all lines are busy and we will get to you as soon as possible".

A spokesman for the Ambulance workers union (NUPE) claimed that the cause was due to a combination of undermanning and the implementation of a new computerised call handling system. He accused the computerised system of "just losing calls in the system". He also claimed the number of deaths in north London became so acute that the computer system was withdrawn. A spokesman for the Ambulance service indicated that they are going through the normal number of "teething troubles" that one gets when introducing any new system or techology, and no one had anything to worry about. When the system was working properly in about 6 months all calls will be handled within 30 seconds. At that point we can rely on a computer system that is 100% reliable and safe.

[Moving off of computers here] When Challenged about the long waits for calls to be answered, he agreed that they were occurring. He said that the Ambulance service must run like any other business and compared it to the Bus and Rail services. He pointed out that he could no more be expected to answer all the calls at peak times than those other services could. The phrase "businesses operating economically and efficiently" was mentioned more than once. He also blamed the public for calling them too much and clogging the lines.

In the light of my recent comments on the media let me note that this program was probably prepared in the wind up to the recent General Election and held in the can as being too "political".

My worries: there is a chance that some computerised systems will not be seen as safety critical, but rather as mundane and ordinary. This might be particularly the case (where in the UK) there is a movement to stop some public services being seen as "special" and to run them like "any other commercial entity". No special care will then be taken in their commission. Others may make other interpretations. I found it hard to document this in a politically neutral way.

Brian Tompsett, Computer Science, University of Hull

### Re: FBI wiretaps (Karn, <u>RISKS-13.41</u>)

Eric S. Raymond <eric@snark.thyrsus.com> 17 Apr 92 05:06:16 GMT

In the middle of a long, thoughtful post on the proposed FBI wiretap bill, Phil Karn made a point which I think can stand some elaboration. In social as well as physical systems, there is no action without equal and opposite reaction.

In considering the cost/benefit of \*any\* law which trades off a loss of privacy and personal freedom against the suppression of criminal activity, we need to evaluate the countermeasures available to criminals. Often, these countermeasures render the law ineffective --- so that honest people are left to suffer only the costs and never see the anticipated benefits.

The proposed wiretap bill clearly has this defect. The facilities the FBI wants to mandate can be defeated with inexpensive end-to-end encryption devices. Thus, supporters of the bill can only maintain their position and the FBI's advantage by intending to ban such encryption devices.

I don't propose to address the damage to our civil liberties that would entail just now, nor the dangerous precedent it would in turn set, except to opine that I would \*far\* rather live with whatever percentage of criminal activity

wiretaps could theoretically suppress than with the potential for systematic governmental mischief implied by wiretaps and encryption bans.

The argument I prefer to make here is that a ban on encryption devices would itself have the same \*pragmatic\* defects as the wiretap bill. Prohibition does not work; criminals would still use and sell encryption devices, and only the honest would be exposed to government error and malice.

It is all too easy to imagine the wiretap bill as the beginning of an action/reaction spiral in which each further encroachment upon the liberties of honest people is `justified' by criminal adaptations to the last one.

If you consider this implausible, take a moment to consider the disastrous histories and perverse effects of gun control and the "war on drugs". We have seen this cycle before. Let's not start another one.

Eric S. Raymond = eric@snark.thyrsus.com (mad mastermind of TMN-Netnews)

# Ke: Intercept legislation (Parker, <u>RISKS-13.41</u>)

Bob Weiner <rsw@cs.brown.edu> Fri, 17 Apr 92 12:53:07 -0400

Your article to RISKS suggests that the FBI's proposed legislation to provide unsecure hooks in telecommunications equipment is necessary to prevent serious crime. Could you explain to the readers how such legislation will help the FBI intercept calls that are encrypted at the transmitting phone and decrypted at the receiving end, which one would assume serious criminals could easily equip themselves with?

If it can, then I buy your point. If it can't, then one has the clear possibility of abuse without the clear possibility of utility in the most serious cases.

Bob

# Ke: Intercept legislation [response to Bob Weiner]

"Donn Parker" <donn\_parker@qm.sri.com> 17 Apr 1992 13:59:53 U

Thanks for your inquiry. Criminals' use of crypto is a separate problem from the intercept issue. It was addressed by the ill-fated DOJ-sponsored Senate bill S266. Easily obtained crypto products will provide a new absolute right of privacy of communication that will obviously be used by some criminals--probably the worst ones. However, the court-ordered intercept will still be of great use for clear text criminal communications. I have interviewed over 150 computer criminals and find many of them to be pretty dumb, lazy, and not very careful some of the time. For example, consider how dumb Gotti and his pals were to have their conversations compromised even when they knew the Feds were intensely investigating them. Therefore, I conclude that there will still be many communications among and from suspected criminals in the clear for which the intercept capability will be valuable. Donn

### K Credit-card fraud

<[anonymous]> Fri, 17 Apr 92 14:40:05 PDT

Computer hackers slick at credit card fraud, say police (by Bruce V. Bigelow and Dwight C. Daniels, Copley News Service)

SAN DIEGO An electronic web of young computer hackers who use high-tech methods to make fraudulent credit card charges and carry out other illegal activities nationwide has been uncovered by San Diego police.

The informal underground network has been trading information "to further their criminal careers," said Detective Dennis Sadler. The hackers know how to break computer security codes, create credit card accounts and make fraudulent credit card purchases, among other things, he said. "These kids can get any information they want on you. Period," said Sadler, who works in the San Diego Police Department's Northern Division. "We didn't believe it until it was demonstrated to us." As many as 1,000 "hard-core" hackers across the United States have shared such data, Sadler said, although it's unclear how many have actually used the information to commit crimes. "It's been going on for at least four years," he said. He estimated that illegal charges to credit cards could total "millions of dollars." Computer criminals "don't go out and charge a thousand dollars every day," Sadler said. "But they have the access and the means to do it any time they want."

A crucial break in the case occurred late March, said Sadler, when an out-of-state hacker was picked up in San Diego and agreed to cooperate with police and the FBI. Detectives brought the hacker to a San Diego computer store that has provided equipment and technical assistance to authorities, according to a source familiar with the investigation. Sadler refused to discuss details, however, saying that the investigation is continuing. Scores of arrests are pending nationwide, he said.

In recent months, the investigation has led to two arrests in Ohio and the seizure of computers and related material in New York City, the Philadelphia area and Seattle. Yet, Sadler said, those cases represent only an "offshoot" of the main investigation.

A San Diego hacker who was questioned by authorities says the case appears to be as big as "Operation Sun Devil," a continuing federal investigation into computer crimes that prompted raids in San Diego and 11 other cities almost two years ago.

Typically, fraudulent credit card charges are racked up by computer criminals who illegally gather detailed information from computerized accounts on file at credit reporting agencies, banks and other businesses.

Electronic trespassers can use a credit card holder's name, address and other personal information gleaned from account files to fraudulently verify purchases, a crime known in hacker vernacular as "carding." Such methods make catalog purchases by telephone a cinch. Smooth-talking hackers have even acquired haircuts and meals by verifying their credit card purchases with personal information, Sadler said. "There's one kid who bragged about using the same credit card number for eight months," Sadler said. The hackers have learned how to break personal security codes for automatic teller machines, Sadler said. Further, using computers, hackers can employ a variety of techniques to obtain long-distance telephone access codes and illegally make telephone calls without paying. "People don't realize what's going on out there," Sadler said. "If you did, you'd shred your credit cards."

MasterCard International reported total losses of \$381 million from credit card fraud of all types worldwide in 1991, according to Warner Brown, MasterCard's director of security and fraud control in Los Angeles.

Losses at Visa International amounted to \$259 million in 1989, about one-tenth of a percent of Visa's worldwide sales volumes, said Gregory Holmes, a Visa spokesman in San Francisco.

American Express has a policy against revealing the extent of its fraud losses, a spokeswoman said.

No figures are available on how much credit card fraud is committed by hackers. "I wouldn't even hazard a guess," said Spencer Nilson, who publishes a bimonthly newsletter in Santa Monica, Calif., about the credit card industry.

Customers don't learn about a fraudulent purchase until they get billed, and any overcharges are disputed for three to six months, Nilson said.

At least part of the investigation is focused on credit information gathered illegally by computer from Equifax Credit Information Services, a credit reporting agency based in Atlanta.

"We're still in the process of investigating, and we're working very closely with San Diego police," said Tina Black, an Equifax spokeswoman. The company, which provides credit information to lenders, is notifying consumers whose accounts were compromised, Black said. Equifax suffered no financial losses itself, and Black could provide no information about possible losses to consumers. "Right now, it looks like only a few," probably fewer than 25, she said.

Equifax disclosed in February, however, that a different group of hackers, including two teen-agers from Kettering, Ohio, had infiltrated its computer, using an Equifax customer number and password code to obtain credit information and bill-paying histories of Midwestern consumers. The two juveniles, who were not identified, face federal and state charges stemming from the computer break-in, said Kettering police spokesman Jeff Caldwell.

Equifax computer experts are checking to determine if computer trespassers created phony consumer files in the agency's mainframe computer.

Equifax, one of the nation's three largest credit bureaus, had revenues of \$1.1 billion in 1991 and possesses a database of about 170 million credit files.

[An AP version of this story appeared on the front page of the San Francisco Chronicle, 18 Apr 1992]

#### Harper's article on Personal Data for Sale

<[anonymous]> Wed, 18 Mar 92 12:49 EST

Harper's Magazine, March 1992, p.21

[Brochure] FOR SALE: DATA ABOUT YOU

(From a sales brochure distributed in 1990 by Nationwide Electronic Tracking (NET), an information-brokering company located in Tampa, Florida. Last December the FBI identified NET as the center of a nationwide organization that illegally obtained and sold information, stored in government computers, about private individuals. According to the FBI, NET paid employees of federal agencies, including the Social Security Administration and the Secret Service, to procure records from various computer networks that are easily accessible to thousands of government workers. The accessed networks included the FBI's National Criminal Information Center, private credit-reporting systems, and the Social Security Administration on about 200 million Americans.)

In our complex, fast-moving society, information is a constantly changing resource. Every day billions of records and documents, containing information on millions of people, must be revised and updated. Sorting through it all for the one particular bit of information you need can be time-consuming and expensive--a frustrating series of false starts, dead ends, and legal barriers. Unfortunately, getting reliable information, and getting it quickly, can often mean the difference between success and failure.

Nationwide Electronic Tracking (NET) can get the information you need--when you need it. NET is a high-speed, computer-based telecommunications network, designed to gain instant access to difficult-to-obtain "confidential" information from more than 1000 sources nationwide. Credit-bureau reports, Social Security searches, electronic cross-directories, and criminal, motor-vehicle, and driving records are just a few of the kinds of information NET can obtain faster than the competition.

#### GUIDE TO SERVICES

#### HOME ADDRESS

PROVIDES SOCIAL SECURITY NUMBER With name and address, will conduct nationwide search for Social Security number.

2 hours, \$10

# SOCIAL SECURITY NUMBER PROVIDES HOME ADDRESS With Social Security number, will obtain name and home address. 1-2 hours, \$7.50

RESIDENT IDENTIFIER Gives names of current residents at a given address. 1 hour, \$10

#### STREET ADDRESS

OF POST OFFICE-BOX RENTER With subject's name, box number, city, state, and zip code, will obtain renter's street address.

1-2 weeks, \$50

#### NATIONAL NEIGHBOR UPDATE

With subject's name and address, will obtain names, phone numbers, and addresses of up to nine current neighbors.

#### 1-2 hours, \$10

#### EMPLOYMENT SEARCH

With name and Social Security number, will obtain current place of employment.

1 week, \$75

#### EMPLOYMENT HISTORIES

With name and Social Security number, will obtain recent places of employment and subject's earnings.

last three years: 3-5 days, \$100 last five years: 3-5 days, \$120 last ten years: 3-5 days, \$175

#### WORKMEN'S COMPENSATION CHECK

(FLORIDA ONLY)

With subject's Social Security number and last known address, will obtain any claims filed.

24 hours, \$75

CREDIT REPORT

Subject's credit history.

1-2 hours, \$10

#### MOTOR VEHICLE INFORMATION

With title number, vehicle number, or license plate number, will obtain name and address of owner, make of vehicle, and license plate number.

Florida, Texas, or New York: 1 hour, \$10 all other states: 2-4 days, \$20

### DRIVER'S LICENSE RECORD

With driver's license number, will obtain home address, traffic violations, and DUI [Driving Under the Influence] charges. We can also obtain information with only individual's name and date of birth; add three days and \$30 for this service.

24-48 hours, \$15

#### **CRIMINAL HISTORY**

With name, date of birth, sex, and race, will obtain criminal history. 1 week, \$100

## SURVEY: Is Big Brother Watching You?

Lorrayne Schaefer <lorrayne@smiley.mitre.org> Fri, 17 Apr 92 07:51:03 EDT

SURVEY: MONITORING IN THE WORKPLACE

The purpose of this survey is to collect data for a presentation that I will give at this year's National Computer Security Conference in October. I would like to thank you for taking the time to fill out this survey. If you have any

questions, you can call me at 703-883-5301 or send me email at lorrayne@smiley.mitre.org. Expand white space as needed [squeezed for RISKS to save paper], and please send your completed survey to:

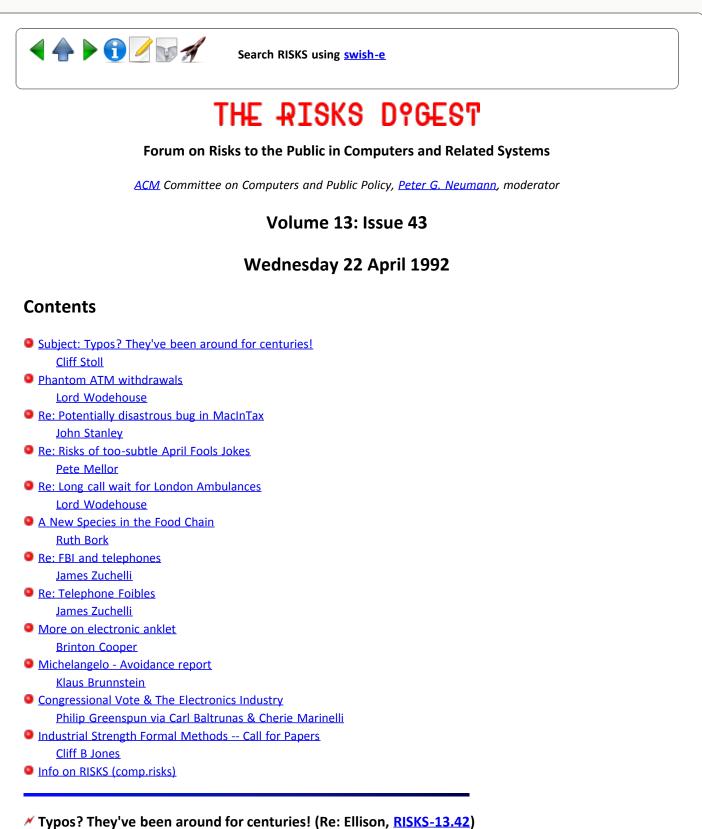
Lorrayne Schaefer The MITRE Corporation M/S Z213 7525 Colshire Drive McLean, VA 22102 lorrayne@smiley.mitre.org (Lorrayne Schaefer)

- 1. What is your title?
- 2. What type of work does your organization do?
- Does your organization currently monitor computer activity? (Yes/No)
- a. If yes, what type of monitoring does your company do (e.g., electronic mail, bulletin boards, telephone, system activity, network activity)?
- b. Why does your company choose to monitor these things and how is it done?
- 4. If you are considering (or are currently) using a monitoring tool, what exactly would you monitor? How would you protect this information?
- 5. Are you for or against monitoring? Why/why not? Think in terms of whether it is ethical or unethical ("ethical" meaning that it is right and "unethical" meaning it is wrong) for an employer to monitor an employee's computer usage. In your response, consider that the employee is allowed by the company to use the computer and the company currently monitors computer activity.
- 6. If your company monitors employees, is it clearly defined in your company policy?
- 7. In your opinion, does the employee have rights in terms of being monitored?
- 8. In your opinion, does the company have rights to protect its assets by using a form of monitoring tool?
- 9. If you are being monitored, do you take offense? Managers: How do you handle situations in which the employee takes offense at being monitored?
- 10. What measures does your company use to prevent misuse of monitoring in the workplace?
- 11. If an employee is caught abusing the monitoring tool, what would happen to that individual? If your company is not using any form of

monitoring, what do you think should happen to an individual who abused the tool?

12. Is it unethical to monitor electronic mail to determine if the employee is not abusing this company resource (e.g., suppose the employee sends personal notes via a network to others that are not work related)? Why or why not?





# Typos: They ve been around for centuries: (ne. Ellison, mo

Cliff Stoll <stoll@ocf.Berkeley.EDU> Mon, 20 Apr 92 20:46:30 -0700

Well, you sure don't need a computer to make typos.

1562 - Geneva bible Matt. v, 9 reads:

"Blessed are the placemakers: for they shall be called the children of God." (oughta be peacemakers)

- 1653 Cambridge printer screws up I Cor. vi, 9:"know ye not that the unrighteous shall inherit the Kingdom of God?
- 1691 Barker & Lewis in London printed a bible with the seventh commandment,"Thou shalt commit adultery."(they were fined 300 pounds and went out of business)
- 1702 London firm prints bible with Psalms cxix, 161: "Printers have persecuted me" (should be "Princes..."
- 1716 First bible printed in Ireland has John v, 14 as: "sin on more" (instead of sin no more)

Things might have improved since then. But maybe not...

[No. Now it would be "Blessed are the pacemakers." By the way, Pete Mellor <pm@cs.city.ac.uk> sent in a further collection, not included here, but suggested that this subject be moved to rec.humor. I agree with him. No more typos unless really RISKS relevant, e.g., life critical. PGN]

### Phantom ATM withdrawals

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 21 Apr 92 14:35:00 BST

The state of affairs in the UK with the banks over "phantom" withdrawals from ATMs is still unresolved. However recently the Abbey National PLC have suffered a spate of thieves driving up with a JCB and removing completely the ATM from the branch office. The last one got away with about 60,000 pounds. They strike at about 4am and they normally have stolen the JCB as well from a local building site. (By the way any puns made on the basis that the Abbey National was once a building society are too "awefull" to mention.)

Lord John - The Programming Peer.

#### Ke: Potentially disastrous bug in MacInTax (Knapp, <u>RISKS-13.42</u>)

John Stanley <stanley@skyking.OCE.ORST.EDU> Mon, 20 Apr 1992 03:20:03 GMT

As a user of another ChipSoft product, I am not surprised.

\_TurboTax\_ provides absolutely no way to indicate that a distribution from a retirement plan that was rolled into an IRA, yet is shown as taxable in the 1099's, should not be taxable income, other than changing the data on the 1099.

This is not the more serious error. Unknown codes on the 1099's cause \_TurboTax\_ to lose track of income that really should be taxed. There is a

warning notice (shown without the "\*" that marks "serious" problems), but none of the codes that \_TurboTax\_ DOES know about cause it to handle this information properly. The only apparent solution is to delete the offending 1099 and enter the numbers in a fake w-2.

Is this a risk of computers, though, or a risk of the overly complex tax codes, which cause some less than competent accountants to report sales of stock as "self-employment" income, which TurboTax quite happily calculates self-employment tax on? Or is it truly a risk of computers, and software authors who assume that nobody needs anything but codes 1-7 and A-B defined for 1099's?

### Ke: Risks of too-subtle April Fools Jokes (RISKS-13.37)

Pete Mellor <pm@cs.city.ac.uk> Tue, 21 Apr 92 13:45:59 BST

One year when April 1st fell on a Sunday, the UK national Sunday paper The Observer carried a story about a proposed new method of operating London buses without drivers. Each vehicle would be fitted with a video camera in the cab, and the images would be relayed to a control centre where, with the aid of a computer control system, one controller would "drive" up to seven buses remotely, sitting in front of a bank of monitor screens on which the view of the road ahead of each bus would be displayed.

I was a bit cross when I got to the end of the article and realised that I had been taken in. However, having seen some of the serious proposals for "drive-by-wire" cars, I think that maybe I was being too hard on myself! :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V OHB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

### Ke: Long call wait for London Ambulances (Tompsett, <u>RISKS-13.42</u>)

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 21 Apr 92 14:50:00 BST

One point not made by Brian Tompsett in his contribution was the problem of a single event generating multiple calls. The controller stated that often a single accident in central London could generate 30 calls to the control room. Each one of these needed to be screened, as until this is done, no one can know if the call is new or old. With eleven staff on duty, it is no surprise that the system fails to cope, as the operator must stay connected to the caller until it is confirmed that an ambulance has been despatched to the scene. With this sort of system, any problem can quickly overcome the reserves in the system and thus leave the new callers "trapped" talking to the BT operator, who is listening to the recorded message.

The computer system should allow for faster despatch, but again the problem is the number of vehicles available at the time. The solution of many more operators does not solve the problem when costs are constrained, so what is needed is a method of clearing through the calls fast to get rid of the duplicates. I am aware of this myself, having recently called the Fire service, having seen a car on fire, and not been the first caller. However I needed to call, because I could not tell if anyone else had reported the problem, and I did not want to ignore it in case everyone else had ignored it too.

Lord John - The Programming Peer.

#### A New Species in the Food Chain

<OHS@northeastern.edu> Mon, 20 Apr 1992 22:11 EST

Many risks, and in such a short announcement; I quote from our local Johnnie's Foodmaster grocery-chain store advertisement:

Charlestown, MA (April 27th, 1992)--Foodmaster Supermarkets is pleased to announce a new electronic payment system to be used for making purchases at three Foodmaster stores.

Foodmaster is excited to be the first in the area to offer this new service to its customers. Any customer who has a Yankee 24(R), BayBank or X-Press 24(R) [ATM] Card can utilize this system. The customer at the point of checkout simply passes their card through the magnetic reader located at the checkout and punches in their secret I.D. number and the transaction is automatically processed.

Foodmaster is pleased to be working in conjunction with Yankee 24, BayBank and Manta Systems, a division of BUYPASS [a sad play upon words]. This new service will be available in...stores in the month of April."

Although the language carefully and slightly hints otherwise, I assume the service is optional (or perhaps the copy writer is prophetic). The usual obvious risks apply, such as PIN protection (both external and internal), sale to others of both the customers' names and/or their buying-habits and multi-bank information (remember the Denver supermarket note a few RISKS issues back?), etc. However, there is now a new twist: banks, \_never\_ tiring of riding herd on their yet-to-succeed debit-card pursuits, are now putting this pressure on with attractions via one of the consumer's most vulnerable points, viz., the basic staple of food. I wonder if supermarket check-cashing will shortly become more "complicated"....

Ruth Bork OHS@NUHUB.ACS.NORTHEASTERN.EDU

#### Re: FBI and telephones (<u>RISKS-13.41</u>)

Tri-Valley Macintosh Users Group,UG <TMUG@applelink.apple.com> 20 Apr 92 08:16 GMT

It seems rather frightening that the FBI needs to be able to monitor the telephone conversations of any individual in the nation at any time. In their

zeal to protect us from criminals they seem to be intent on being able to snoop without warrant or reason.

Further, from my reading of the bill, encrypted messages could be included in the list of forbidden technology. Wouldn't this please the NSA?

Has the FBI done any type of study that shows there is a wholesale use of the telephone system by criminals or is this merely a smoke screen to enable the federal police to have the ability to monitor any individual or group at any time.

What happens when non-governmental persons learn of the access techniques. If the entire nation's phone system is set up so it can be tapped, then no conversation can be considered secure.

This proposed law sounds like a terrible abuse of power by the FBI. Until they can show some valid reason for having the ability to tap every conversation in the country this bill should be tabled.

Furthermore, from what I have read over the years, the equipment is already available to enable the government to tap any phone anywhere whenever they want to.

James Zuchelli

### Re: Telephone Foibles

Tri-Valley Macintosh Users Group,UG <TMUG@applelink.apple.com> 20 Apr 92 08:04 GMT

The alternate phone company was located in Texas. They assumed that it was toll fraud call and credited me for the calls. Michigan Bell said that my local phone company (Pacific Bell) would have to investigate if it was a fraudulent call. Pacific Bell said they wouldn't do anything about it.

I got the number where the calls were billed from, from the alternate carrier and tried to call it, but the call would not go through. A Michigan Bell operator said the phone booth was set up to only send calls out, no incoming calls would be accepted. She said that \*\*\* a nationally known company is located in Ada and one of their employees probably made the call, but offered no explanation as to why someone who might have stolen my card number would only make two calls.

When I pointed out that public phones that won't take incoming calls are usually located in high crime areas, the operator seemed surprised. I got the feeling that there are a lot of fraudulent calls made from Ada.

If I ever can find out exactly what happened I will relay the info to Risks Forum.

James Zuchelli

# More on electronic anklet (Re: <u>RISKS-13.38</u>)

Brinton Cooper <abc@BRL.MIL> Thu, 16 Apr 92 0:14:54 EDT

Subtitled: Risks of Quote without Comment

<u>RISKS-13.38</u> quotes AP from Paterson, NJ, that a drug offender under house arrest killed another man after a computer error enabled him to break his electronic anklet and leave the house. The risk in such a posting, without some sort of qualifying comment is to seem to endorse the notion that society should not use electronic, computer-controlled house arrest systems because the "prisoners" can break away and commit murder.

At some point in our evolving history, we need hard information (hard to come by?) comparing the risks to society of electronic house arrest vs

- 1. having to set some prisoners free because the jails are full;
- cramming more prisoners into fixed-size jails, thus ensuring their everlasting rage and resentment, fixing forever what mental ills brought them there in the first place so that, when they finally serve their sentences, they'll kill someone with probability one;
- taxing law-abiding citizens ever more heavily to build more jails to house the criminals, thus increasing everyone's resentment levels, pushing more "over the edge," creating yet more criminals.

If our interest in the failure of electronic house arrest monitors is purely scientific/technical, if such postings are made only so that we can discuss how to make such systems more robust and less susceptible to overload, then, once in a while someone should say so.

Well, I may have overreacted, but I think it needed to be said.

\_Brint

#### Michelangelo - Avoidance report

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de> 8 Mar 92 13:27 +0100

[An old item. I meant to run it sooner, when it was timely, but it is still relevant. PGN]

In Germany, early warnings and high press activity helped to avoid data loss on March 6, 1992. From the German CERT's (Computer Emergency Response Teams, as installed by German Information Security Agency, GISA, similar to US centers as organised by CMU), including MicroBIT Virus Center, Technical University of Karlsruhe (Christoph Fischer), Virus Test Center, University of Hamburg and GISA itself, the following figures have been given:

- Between Jan.1st and March 5, 1992, about 1,000 cases of Michelangelo had been reported to one of the centers. Roughly estimated, about one third each came from individuals, small enterprises and medium to larger enterprises. As a rough estimate, these 1,000 reports (mostly via telephone asking for advice after detection) represent about 5-10,000 PCs.
- On March 5, 1992, the first accident was reported to VTC; a local enterprise followed some press advice to change the date. In order to avoid March 6 the next day, they changed the date to March 6 at afternoon of March 5, evidently without checking for Michelangelo. After some reset, Michelangelo hit one PC. Moreover, there were rumors that some PCs had suffered from Michelangelo as Feb.29 1992 was not available on their PCs.
- On March 6, 1992, about 50 cases were reported in the 3 centers; apart from individuals, small enterprises called but no large ones. This low figure may be slightly too low as telephone lines were busy most of the time with media asking for recent data; in VTC, we had even a TV team waiting for accident reports to come in.

>From the media point ov view, the warning was inadequate as nothing happened. This view was assisted by some "experts" such as Chaos Computer Club that the press reports and warnings were essentially advertisements for Hannover fair's next week beginning CeBit (world's largest exhibition in IT), and to assist antivirus industry. CCC's representative Mr. Steffen Wernery even argued that the virus should not been named "Michelangelo" but after one warner (myself), and that the only 100 viruses (sic; in VTCs database, we presently have 1,200 viruses) are no real danger!

>From the warner's point of view, the warning was successful as it probably avoided accidents. But as is usual since ancient times, the messenger is punished for the warnings - I was even asked whether I received more invitations for lectures etc (I did not).

After we first informed the public (German press agency, DPA, end-of-January), VTC received more than 6,000 telephone calls (as recorded by university telephone computer), most of them asking for general antivirus advice.

MicroBIT (Christoph Fischer) and VTC both (Morton Swimmer) produced and distributed (free-of-charge) special aNTI-MICHelangelo programs easy to use which also detect and diagnose possible variations of date (not yet detected). When we informed the public (via DPA etc) about availability of NTIMICH (on Friday 21, 1992), we received about 18,000 diskettes with prepared envelopes. My students copied 14,000 diskettes (they even found viruses on some diskette sent, esp. Stoned, Michelangelo), the rest being copied and distributed by Siemens-Nixdorf (SNI) which kindly assisted us. All diskettes were sent back until Wednesday March 4, 1992. Moreover, NTIMICH was available from FTP, mailboxes, BTX and even from some radio/TV stations. In addition, a German TV magazine (1st channel: WISO, specialized in economic and social features) dis tributed 100,000 copies of McAfee's Scan at low price (2 DM) via consumer organisation's offices.

As a SUMMARY, this was probably the first time that many users and enterprises had prepared some data backup and practices some antivirus methods.

Consequently, many other virus (Stoned, Cascade/170x, Jerusalem/Isreali/Friday 13) were also detected and eradicated. Moreover, public attention was drawn to inherent insecurity of PCs.

Some CONSEQUENCES will follow: some users who bought PCs with installed Michelangelo or on some diskettes (mouse, VGA drivers etc) think of prosecuting the resp. dealers. Some PC dealers (and hopefully some software houses) have installed improved methods of quality (e.g. virus testing on golden master).

Many now ask for improved LEGISLATION to prosecute virus authors. This will be very difficult as those countries with presently most productive virus factories (Bulgaria, Taiwan, Former Soviet Union) lack any legislation about copyrights or computer criminal acts. For US and European prosecutors, it will be impossible to prosecute the (probably Taiwanese) authors of the original Michelangelo virus (detected in Australia 1990, with a text on Michelangelo's birthdate replacing the usual Stoned text) or those (probably European) authors which updated the original version not to contain any detectable text (this version now found in Europe, USA and Africa was detected in March 1991 in Sweden and Netherland; both countries have no adequate legislation).

Klaus Brunnstein, University of Hamburg, March 8, 1992 (13:00 pm German time)

#### Congressional Vote & The Electronics Industry

Carl Baltrunas & Cherie Marinelli 1.5v4 <carl@udwarf.tymnet.com> Sat, 18 Apr 92 03:42:26 PDT

I had this article forwarded to me and since I had not seen anything in RISKS about this particular congressional vote, I thought it might be of interest to other risks readers. -Carl

----- Forwarded Article from misc.legal.computing

Date: 17 Apr 92 19:32:31 GMT From: philg@zurich.ai.mit.edu (Philip Greenspun) Newsgroups: misc.legal.computing Subject: US Congress votes to subsidize Japanese electronics industry Message-ID: <PHILG.92Apr17153231@orion.ai.mit.edu>

In the decades to come, every American computer user who purchases floppy disks will pay a tax. Most of the money collected will go to record companies owned by foreigners, notably Sony, Philips and Matsushita. Congress, after receiving substantial campaign contributions from the recording industry, has decided that Americans are criminals who don't want to pay for CDs. Therefore digital audio media such as DAT tapes and writable optical disks will be taxed and the money handed over to record companies and artists. Just as consumer DAT and 8mm video tape have become the standard high-capacity backup media for workstations/minis, it is likely that writable optical digital audio disks will replace today's magnetic floppy disks. Sony and Matsushita own two of the largest record companies in the US and would get the most money from this bill. Two years from now, every time American users of IBM computers make a backup, they'll be paying a tax to help out IBM's Japanese competitors. Additional reasons to dislike this bill are varied. It will be illegal to sell consumer digital audio recorders in the US that can make digital-to-digital copies after one generation. You'll pay a tax on your shiny new Japanese machine, you'll pay a tax on the tape and when you try to assemble a recording of your own music, all you'll get is a big flashing "you are a criminal sign." You'll have to spend \$5,000 on a "professional" machine in order to gain any real benefit from the new products. Congress is creating a new government bureaucracy to administer the tax collection from Americans and subsequent distribution to foreign-owned record companies. Manufacturing digital audio equipment will now require hiring a lawyer to wade through over one hundred pages of legal requirements and technical specifications, thus hindering small American companies in competing with large foreign ones. Finally, now one seems to have considered whether this will "promote the progress of the arts", which is the constitutional justification for expanding copyright. Since the money is distributed linearly according to sales, only the biggest record companies and most popular stars will get any significant money.

You can stop this bill from passing. Congress is sticking it to us because the recording industry paid them and they don't think anyone will notice. CSPAN and most newspapers haven't covered this issue at all because the bill has dozens of co-sponsors and is therefore considered non-controversial. If a Congressman gets even a few letters regarding this bill, which he's probably hardly thought about at all, it might be enough to make him think that subsidizing Japanese computer vendors isn't such a great idea. The bill is going to be voted on in about two weeks. It is called the "Audio Home Recording Act of 1991" and is S-1623 in the Senate and HR-3204 in the House. You can write to your elected representatives this way:

Senator Foo Bar The Capitol Washington, DC 20510

Representative Foo Bar The Capitol Washington, DC 20515

If you want any more information, please feel free to contact me (philg@altdorf.ai.mit.edu). I testified before the relevant Senate subcommittee last Fall as the "nerd witness from MIT."

----- End of Forwarded Article from misc.legal.computing

PS: I make NO claim for the accuracy of this article. Please contact the author as listed in the mail header for more information. -Carl

Carl A Baltrunas - Catalyst Art Cherie Marinelli - Bijoux Internet: carl@udwarf.tymnet.com, carl@udwarf.UUCP carl@tymnet.com cherie%udwarf@tardis.tymnet.com UUCP: uunet!oliveb!tymix!udwarf!{carl or cherie}

[I include this in RISKS with some trepidation. Recognizing that RISKS is a truly international medium and that this message is quite nationalistic, I anticipate some other opinions -- although I would like to see them primarily

on the potential impact on computer usage (not on the Japanese competition issue or whether to feed the artists, which are well beyond the scope of RISKS). PGN]

### Mindustrial Strength Formal Methods -- Call for Papers

Cliff B Jones <cliff@computer-science.manchester.ac.uk> Mon, 20 Apr 92 13:06:45 BST

> FME '93 SYMPOSIUM "INDUSTRIAL STRENGTH FORMAL METHODS"

Sponsored by the Commission of the European Communities (CEC) Organised by Formal Methods Europe

The first FME Symposium will be held at Odense Technical College in Denmark, during the week of 19 to 23 April, 1993. It is being organised by Formal Methods Europe, as the successor to the last four VDM symposia, to promote the interests of users, researchers and developers of precise mathematical methods in program development.

The last few years have borne witness to the remarkable diversity of formal methods, with applications to sequential and concurrent software, to real-time and reactive systems, and to hardware design. In that time, many theoretical problems have been tackled and solved, and many continue to be worked upon. Yet it is by the suitability of their industrial application and the extent of their usage that formal methods will ultimately be judged. This symposium will focus on the application of industrial-strength formal methods. We encourage all papers to address the difficulties of scaling their techniques up to industrial-sized problems, and of their suitability in the work-place. Papers should discuss techniques that are formal (that is, they have a mathematical basis), and that are industrially applicable. Papers tackling theoretical issues are much encouraged, providing that they contain a justification of the practical advantages that follow.

Full-length research papers, industrial reports, proposals for tutorials and tool demonstrations are solicited, particularly in the following areas:

* Practical use *	Case	studies
-------------------	------	---------

- \* Tools \* Linking formal and informal methods
- \* Comparisons of formal methods \* Proof
- \* Concurrency \* Real-time and reactive systems
- \* Refinement techniques \* Object orientation
- \* Secure systems \* Safety-critical systems
- \* The development process \* Education and technology transfer
- 1 October 1992: Submissions
  - Full, original research papers (6 copies, 12pt, single spaced, max 20pp)
  - Industrial usage reports (6 copies, 12pt, single spaced, maximum 10pp)
  - Proposals for tutorials (half day, maximum 50pp of notes)
  - Proposals for tool demonstrations (with hardware/software requirements)

Proposals for tools demonstrations should be send to the organising chairman, while all other proposals should be send to the programme chairman. Industrial usage reports do not need to conform to usual standards for academic papers.

- 1 December 1992: Notification of acceptance
- 1 February 1993: Camera-ready copy due for publishers

Programme Chairman	Organising Chairman
Jim C.P. Woodcock,	Peter Gorm Larsen,
Oxford University	The Institute of Applied
Computing Laboratory,	Computer Science (IFAD),
Programming Research Gr	oup Forskerparken 10,
11 Keble Road,	DK-5230 Odense M
Oxford OX1 3QD, UK	Denmark
tel: +44 865 272576	tel: +45 65 93 23 00
fax: +44 865 273839	fax: +45 65 93 29 99
email: jimw@prg.ox.ac.uk	email: peter@ifad.dk

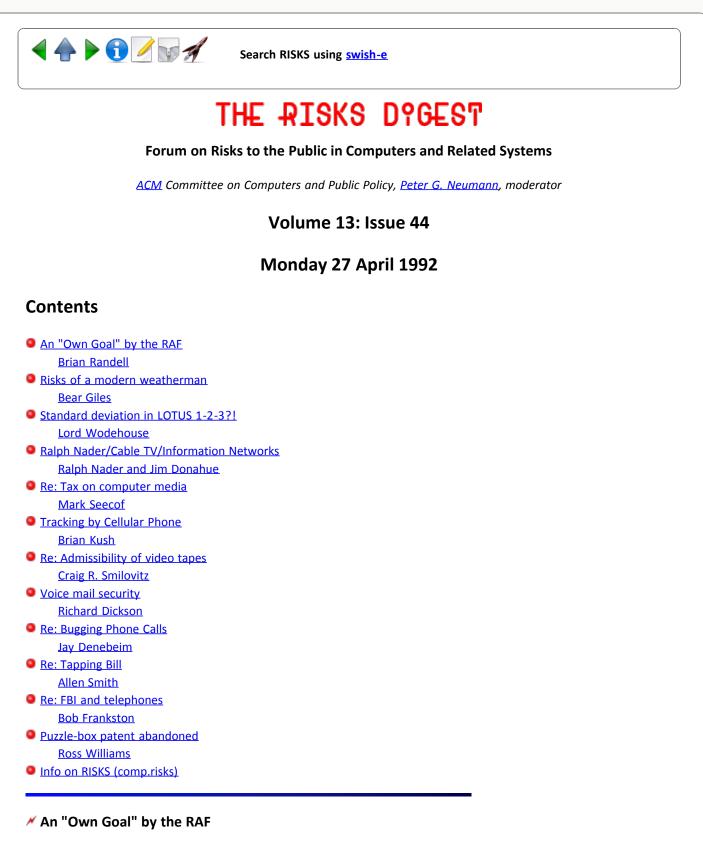
**Executive Programme Committee** 

J.-R. Abrial (F) Tim Denvir (GB) Eugene Durr (NL) Ian Hayes (AUS) Steve King (GB) Hans Langmaack (D) Micheal Mac an Airchinnigh (IRL) Kees Middelburg (NL) Soren Prehn (DK) Hans Toetenel (NL)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<Brian.Randell@newcastle.ac.uk> Thu, 23 Apr 1992 09:28:16 +0000

The following is quoted in its entirety, from the 23 Apr 1992 issue of The Independent, a "quality" UK National Newspaper. Its discussion of how an Royal Air Force Sea Harrier managed to bomb a Royal Navy aircraft carrier is entirely speculative, offering either a computer malfunction, or failure by the pilot to press a button as likely causes. However I find the statement that "offset" bombing practice relies on a simple button press to ensure that the ship towing the target does not itself become the target both interesting and worrying, if true. Brian Randell

`ARK ROYAL' WAS BOMBED BY RAF HARRIER PILOT By Christopher Bellamy, Defence Correspondent

The Royal Navy launched an inquiry yesterday into how a Royal Air Force pilot bombed its most modern carrier, Ark Royal, on Monday, missing the intended target by 500 yards. Navy sources said that one of the two RAF pilots flying with the Royal Navy during the exercise had applied to transfer to the senior service. It is not clear if the incident will affect that move.

The Ministry of Defence said such an accident had never happened before but refused to speculate how the Sea Harrier 1 from Ark Royal missed the target towed behind the ship and, according to the MoD, put the bomb through the flight deck. Six sailors were hurt, one seriously, and five were still in the Royal Naval Hospital Haslar, Portsmouth, yesterday. However, it is almost certain that the plane was practising an attack using the "offset" procedure. It is possible that the RAF pilot of the Navy plane failed to press the button to switch from a reference point - the carrier - to the target. "Offset" is used where the target may be difficult to see, but its position relative to a clear reference point is known.

The practice bomb has the same flight characteristics as a real one but carries only a small explosive charge to mark where it lands. The charge exploded inside the carrier, starting a small fire. Under the offset procedure, the plane's computers make the calculations needed to adjust the bomb's trajectory from the "false" target to the real one.

The Sea Harrier pilot lines up on the ship from about five miles and 250 feet above the water. Flying towards the ship he then tells the computer to attack the "splash target", towed 500 to 1,000 yards behind, while still flying at the ship. The attack must be carried out from the beam, or the computer software will automatically prevent bomb release. At the optimum height, speed and distance the computer tells the pilot to pull up and release the bomb.

Paul Beaver, publisher of Jane's Defence Weekly, said: "It does rely on the pilot to press the button to switch from the mock target to the real one." On Monday, the button may not have been pressed or the computer may have malfunctioned, and the bomb went into the reference point - Ark Royal - instead of into the target. The practice bomb hit the carrier about one third of the way aft of the ski-jump and slightly to port, reportedly penetrating the flight deck and exploding in the mess deck below. But Mr. Beaver said he was "very surprised" to hear the bomb had penetrated the flight deck. At that trajectory, he said, it was more likely to have bounced off - unless it went into the ship's side.

[Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 91 222 7923 FAX = +44 91 222 8232]

### Kisks of a modern weatherman

Bear Giles <bear@tigger.cs.colorado.edu> Wed, 22 Apr 1992 12:54:15 -0600

(From the bulletin board down the hall...)

Network Wind Profiler Severely Damaged

A wind profiler in OAR's Wind Profiler Demonstration Network (WPDN) was severely damaged by several shot-gun blasts late last week. On March 28, just before sunrise, two men and one woman were pheasant hunting in southern Nebraska [and] came across the McCook wind profiler and mistook it for an alien spacecraft. Frightened, they fired a number of shots damaging the profiler antenna and the electronics shed. Furthermore, a Forecast Systems Lab (FSL) technician who was in the shed conducting routine system checks was taken hostage by the hunters. After being held captive for nearly two hours, the technician's partner arrived and explained to the hunters what the profiler really was. The hunters then fled and so far, they have not been apprehended by law enforcement officials. Profiler damage is estimated at \$150,000.

A profiler (developed in the building where I work) is a phase-array radar which "looks" nearly straight up. The basic model can determine wind direction and speed from the ground to about 50 mb (around 20km, at a guess); a recently developed enhancement can also determine air temperature up to the tropopause. They are used in a manner similar to weather balloons, but provided hourly summaries instead of 12-hour reports. (They operate continuously, but the data is rather noisy).

I've never seen an actual profiler on the ground, but the models and artist's conceptions show a flat rectangular grid. Coworkers describe it as a "construction junkyard", or "flat pipes" held about 4 ft above the ground.

Of course, those of us in the mountains have a very low opinion of plains-dwellers. Several meteorologists on a "storm chase" last year reported on Kansan walking up to them (on the side of the road) and asking "Is that a tornado?" What he thought the large funnel cloud a few miles away was, if not a tornado, nobody has every figured out...

Bear Giles bear@fsl.noaa.gov [Yes -- the "fsl" is for Forecast Systems Lab] National Oceanic & Atmospheric Adminstration / Boulder Labs

#### X Standard deviation in LOTUS 1-2-3 ?!

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 23 Apr 92 15:51:00 BST

My company has just sent out in an internal magazine a comment about the @std function in LOTUS 1-2-3. From this I gather that the @std function in both

version 2.2 and 3.1 uses the number in the sample (n) and not the number in the sample - 1 (n-1). Version 3.1 has a second macro to use the correct value. Version 2.2 manual comments that the @std should only be used on large samples. The comment in our magazine defines small samples as less than 30.

Two things arise from this. 1) Just how much work has been done by people using 1-2-3, who have not realized the "error", and 2) why have two versions of the macro, when the correct one works for all samples. (my guess is that if the original incorrect version was changed, users would worry about the different answers obtained after the change, even though the answers would now be "correct".)

Moral: You should never trust blindly answers from any statistical package on a computer, unless you know the formula used by the package.

Lord John - The Programming Peer

#### Kalph Nader/Cable TV/Information Networks

"Essential Information, Inc." <0002633455@mcimail.com> Mon, 27 Apr 92 07:08 GMT

From: Ralph Nader, Washington, DC Date: April 16, 1992

Summary: Your help is needed to secure an amendment to pending cable television legislation. The amendment would create a mechanism to organize local Cable Consumer Action Groups (CCAGs) to represent the interests of consumers directly before regulatory and legislative bodies. This proposal is an innovative way to create countervailing power to some of the large corporate interests that control our information infrastructure, and it is a model that is highly relevant for users of voice and data network services. Readers are asked to sign a letter to Congress supporting this amendment. Action is needed very soon. Respond to Jim Donahue, Teledemocracy Project (Internet: 0002633455@mcimail.com)

#### Dear citizen:

As you may know, congress is currently considering cable television legislation. Every television consumer should be concerned about the outcome of this legislation, and particularly citizens who are concerned about the future of information technologies. The current fiasco with the cable industry is an important example of the management of information technologies for the benefit of a few corporate monopolists at the expense of the many. Today nearly all americans are confronted with a monopoly provider of cable video signals, who not only has total control over what you can receive, but also what you pay.

Over the next 15 years we will see a rapid convergence of information technologies. Soon it will be possible to transmit voice, data, and video signals over the same fiber optic telecommunications infrastructure. The fight

over who will control the content of information that flows over that infrastructure, and how it will be priced, will define who can send and who can receive information in digital form. As the use of modern technologies increasingly makes it easier to meter the consumption of information products and services, the gaps between the information rich and information poor will continue to grow.

The current battle over the regulation of the cable television industry is an important step in a more general battle over the control of our information infrastructure. This is a battle over power and wealth, and also over democratic values, competition, and enlightenment. Will we harness our great new information technologies to promote a diversity of sources of information, or will these technologies be used primarily as vehicles for narrowly focused commercial interests, exercising monopoly power?

#### CABLE CONSUMER ACTION GROUPS (CCAG) AS COUNTERVAILING POWER

A number of consumer groups have asked Congress to adopt an innovative proposal to help cable television subscribers organize to represent their interests. Notices describing local Cable Consumer Action Groups (CCAGs), which would be independent and democratically controlled local organizations, would be placed in the cable companies billings. The notices describe the purposes and goals of the group and solicit funds for membership. The CCAG would be required to reimburse the cable company for the incremental costs of inserting the notice in the bill, so the cost would not be a burden to the cable company or its subscribers. These local subscriber consumer groups would then monitor the policies and practices of the cable company, and represent consumer interests in regulatory and legislative proceedings and with the cable companies directly.

The cable industry is extremely active politically, contributing millions of dollars to candidates for political office and spending millions more in lobbying activities before legislative and regulatory bodies. In the absence of something like the CCAG, important public policy issues are debated in an extremely unbalanced way. The CCAG is a modest but important step in addressing a very corrupt system that regularly tramples on the rights and interests of consumers.

Among the groups that have endorsed this proposal are:

Center for Media Education Consumer Federation of America New York City Commissioner of Consumer Affairs Public Citizen Teledemocracy Project U.S. Public Interest Research Group

#### HAS IT BEEN TRIED BEFORE?

This proposal is based on the highly successful Citizen Utility Board (CUB) model, which has represented ratepayers in several states. The most successful CUB, in Illinois, has 170,000 members; its advocacy has saved consumers some \$2 billion over the past several years. Other CUBs exist in Wisconsin, Oregon and San Diego. We want to see this innovation used nation wide in the cable

television industry. (Of course, it may well be a model that has applications to other telecommunications issues.)

#### WHAT YOU CAN DO

The CCAG proposal was included in H.R. 4850, but was deleted by a voice vote (in contrast to a recorded vote) in the House Subcommittee on Telecommunications and Finance. The bill is now in the full Energy and Commerce Committee, where committee supporters will seek to restore the provision through an amendment. We are asking you to send us an email message giving permission to use your name in a letter to Congress supporting this amendment. If you are willing to do so send the following information to the Teledemocracy Project (internet: 0002633455@mcimail.com, or fax 202-234-5176).

Name: Title: (optional) Affiliation: (optional) Address: City and State: (important, for obvious reasons) telephone: (for verification) email address: optional

Thank you very much for your help on this.

Sincerely, Ralph Nader

[A copy of the letter follows:]

Chairman Edward Markey Subcommittee on Telecommunications and Finance Committee on Energy and Commerce Washington, D.C. 20515

Dear Chairman Markey:

We are writing to support your "consumer representation" amendment to H.R. 4850, the cable re-regulation bill. It is imperative that new cable legislation provide a mechanism that gives consumers a stronger voice in regulatory and legislative debates. This amendment is ideal because it brings citizens into the regulatory process at no cost to the government or the cable industry.

Who in Congress can deny the unfairness of a system where the owners of cable monopolies can use subscriber revenues for lobbying purposes while consumers are left powerless and unrepresented? This is only a small step toward curbing the monopolistic power of the cable television industry. We urge the House Energy and Commerce Committee to include your consumer representation amendment in the cable bill.

Sincerely, ...

[For more information, contact: Jim Donahue, Teledemocracy Project, voice: 202/387-8030, fax: 202/234-5176, Internet: 0002633455@mcimail.com]

[For a an email copy of the amendment contact Jim Donahue (internet: 0002633455@mcimail.com).]

## Ke: Tax on computer media (<u>RISKS-13.43</u>)

Mark Seecof <marks@capnet.latimes.com> Wed, 22 Apr 92 10:22:42 -0700

A tax on clarinet reeds would hit only musicians and reed makers (and indirectly music fans); a tax on gasoline hits just about everyone. A tax on computer media, ostensibly aimed at music consumers, would come to hit everyone because of the simple fact that computers are spreading through society faster than a nasty joke through a frat house. A tax on computer media will soon be as general a tax as one on gasoline. I don't think there's any RISK to computer users in such a tax, except at the same level as the risk to automobile users in a fuel tax. The tax is objectionable because it's a general tax for the specific benefit of an unworthy few; and because the legislators responsible for it perhaps do not understand the full effect of the proposed law. The only REAL problem is that uneducated people are yet unaware of the fact that while 1/4" audio tape and IBM 5081 punch cards were distinctly different, in the modern digitally-recorded computer-processed "information age" it is impossible to distinguish between musical and textual and graphical storage media. At worst, tax avoidance schemes based upon artificially differentiating music media and computer media would add some cost, a little less than the tax itself would, to computer media, and generally reduce the economic efficiency of all digital technology industries.

Mark Seecof <marks@latimes.com>

#### Tracking by Cellular Phone

"Brian Kush" <bkush.US1.oramail@us.oracle.com> Fri, 24 Apr 92 08:00:45 PDT

Yesterday while driving through GA, my Cellular Phone rang. Since I was roaming I was not expecting a call. When I answered it, it was a recording welcoming me to Bell South Mobility and offered instructions on using there service. I have had this happen before and did not think anything about it. Though today I started to think. If the cellular phone company could sense that I had come into there area, they could track my movements all over the country on a carrier by carrier basis. They might even be able to track me with in a city/area by which antenna was picking up my signal.

Right now the risk is rather low, but its something to think about.

Brian Kush, Sales Consultant, Oracle Express, Eastern Region, 412.262.5200 vmail: 412.269.3518 pager: 800-SKY-PAGE PIN# 5773865

Re: Admissibility of video tapes

Craig R. Smilovitz <craig.smilovitz@spd.analog.com> Thu, 23 Apr 92 14:53:23 EDT

There seems to be a strange idea that has been floating around in some of the recent postings on comp.risks: namely, that video tape records of your actions necessarily belong to you and their use in a trial as evidence is an invasion of your privacy.

Events that happen in public places are public knowledge and not private. While recordings (video or otherwise) can not necessarily be used for profit by a third party, they are public and may be distributed and used as evidence. Anyone is allowed to see and to tell about what they see in a public place (such as the street corner on which Rodney King was assaulted). That retelling may include using aids such as a video tape.

Things get somewhat more interesting when talking about a camera mounted somewhere and run without an operator. Then the viewing analogy does not hold as well. In those cases, judging by common practice, there may be some principle in the law dealing with the likelihood of knowing that you are witnessed. When there are people standing nearby, you know that likelihood is great. Locations that have video-tape surveillance tend to have signs advising patrons of that fact.

Hope this is of some help when talking about privacy and videotape. Of course, the definition of a public place can get muddy but in the case of the Rodney King beating video this is not an issue.

**Craig Smilovitz** 

### ✓ Voice-mail security

<DICKSON@krdc.int.alcan.ca> Fri, 24 Apr 1992 08:43 EST

I request you assistance with collecting some information regarding the problem of voice-mail security. I have noticed some previous comms in the risks board re this subject and I would like to collect further info regarding risks of these systems.

Are call loggers a problem when you give your password to a mail retreival system form a hotel or an office. Is there a hacker market for this info? Finally how prevelant is this problem in various parts of the world?

How can we protect ourselves from these problems?

Thank you in anticipation. Responses please to the following address:

Richard Dickson ( DICKSON@KRDC.INT.ALCAN.CA )

N.B. this is a server address and not the address of the phone system in question. So if there are any abusers out there, you'll get no hints from me !

# Ke: Bugging Phone Calls (<u>RISKS-13.43</u>)

Jay Denebeim <Jay@deepthot.cary.nc.us> Sun, 26 Apr 92 12:21:44 EDT

The main thing that bothers me about this bill is, why is it needed? I work for a major vendor of central office switching equipment, and I see absolutely no reason to enact such a law.

At the CO/PBX hosting the line it will always be possible to 'listen' to any of the terminals off that line. This is required for ensuring the equipment is working. I cannot concieve a system where this would not be a requirement.

Looking at the proposed law that was reproduced in a previous issue of RISKS, it appears that what they are asking for is the ability to capture the bit stream from any terminal. No more, no less, it specifically excluded the any responsibility for the telco to unencrypt anything fed to the terminal.

The bit stream from any terminal is available at the CO. It has to be, otherwise it would not be possible to identify which terminal to route the return bit stream to.

Jay Denebeim UUCP: duke!wolves!deepthot!jay jay@deepthot.cary.nc.us BBS:(919)-460-7430 VOICE:(919)-460-6934

#### 🗡 Re: Tapping Bill

<ALLENS@earlham.bitnet> Fri, 24 Apr 1992 10:23 EST

•••

>8 "(2) 'communication' means any wire or electronic

>9 communication, as defined in subsection 2510(1) and

>10 2510 (12), of Title 18, United States Code;

This definition means, unless the other laws cited are such as to modify this interpretation, that they could technically demand that all BBSes, etc. set themselves up so that they could be tapped without their knowledge or consent, and can be fined for not complying with this regulation. I suspect how this might be used would be for the BBS to be informed of this "responsibility" after the FBI/Secret Service/whatever thinks they're doing something they shouldn't (which they might extend to legitimate political activity such as pro-drug-legalization), thus causing them to have massive amounts of fines to pay off.

-Allen

### Re: FBI and telephones (<u>RISKS-13.41</u>)

<Bob\_Frankston@frankston.com> Wed 22 Apr 1992 14:52 -0500 I'm surprised that there has been little mention of traffic analysis. Even if the conversations are encrypted, information about who is calling whom can be very valuable.

#### Puzzle-box patent abandoned

Ross Williams <ross@spam.maths.adelaide.edu.au> 23 Apr 92 15:50:55 GMT

Readers of risks may remember that in mid 1991 I posted a message describing a "puzzle-box" idea, for which I had lodged an Australian provisional patent. [See <u>RISKS-12.06</u> and .07. PGN]

The idea was to place some kind of hardware "puzzle" between computers and the safety-critical/trusted devices they control so as to reduce the likelihood of accidental activation in the case of a failure of the computer or the interface. To activate the critical device, the computer would have to send out a complicated sequence to "solve" the puzzle.

The posting created quite a fuss for the following reasons:

- \* People thought that it was covered by prior art.
- \* People thought that it was too simple to be worthy of a patent.
- \* People were concerned that it could be applied to software.
- \* People thought that the idea would never work because of single point software vulnerabilities.

Except for the last criticism, which was provably (by construction) incorrect, all of these criticisms were valid, although perhaps not as valid as many thought. I was mailed quite a lot of claimed examples of prior art, most of which held some similarity, but none of which hit the mark until I heard about a satellite that had been sent up in the 1980s which had exactly what I would call a puzzle box in the form of a linear shift register puzzle that was protecting a rocket motor (or something equally as important). I never managed to formally obtain the details of this example, but if it was true, it was bang on. As it happened, it didn't matter, as all the hate mail put me off the patenting idea anyway.

Later on in the year I happened across a friend who said that he had been involved in a missile project some years ago that had used some sort of "puzzle box" in between a controller of some kind and a firing mechanism. Apparently, on occasions during lab tests, the computer was not able to fire the puzzle box, and so they would call in a technician who had a box with a bouncy switch that just happened to reliably generate the firing sequence... So much for protection!

Anyway, there are three main points that I want to make. The first is that I have completely abandoned the puzzle box patent. My reasons:

- \* I don't want to own a patent that most people seem to hate.
- \* Although I have not formally checked it out, I have heard of at least one convincing prior art example (the satellite).

The second point is that because my patent has been formally registered in Australia, and publicised, there can be no chance of anyone else successfully sustaining a similar patent. Even if the idea had never actually been written down previously, it is now definitely prior art. (Those who are paranoid about my intentions will be pleased to hear that the provisional patent application has now actually expired so I now can't resurrect the patent, even if I changed my mind).

The third and by far the most important point, and the one likely to be of most interest to risks readers, is this. Despite the huge barrage of mail that I received claiming prior art, almost none of it was in safety critical applications. People claimed particular forms of protected memory, clock chips, even Unix passwords, as prior art, but very few people provided examples from trusted systems.

One of the reasons why I lodged the patent in the first place was because I wanted to use the patent to draw attention to the puzzle box idea. I was involved in safety-critical systems for a year and a half, and during that time I didn't hear of any explicit puzzle box mechanism being used in any safety-critical system. Most of the systems that I saw attacked the interface problem using a battery of non-puzzle-box techniques such as output delay and sampling, multiple processors, and analog voting schemes.

So my question is this: Are puzzle boxes a widely known and used technique in safety-critical applications, or are they not? If they ARE in use, then I am surprised because I haven't heard much of them, and in particular, they didn't turn up in the prior art barrage, even though the patent, and my presentation of it in comp.risks, was entirely directed towards safety-critical applications. If they are NOT in use then I think that it is important that the safety critical community become more aware of them, as they can provide a much needed extra layer of protection. My experience working in the field was that there was too much emphasis placed on the software, and not enough on simple physical checking systems or human procedures that could reduce the criticality of the software. It would seem a shame if my patent, defeated by hate mail and clock chips :-), does not impact on its intended safety-critical audience who are in a position to use puzzle boxes to save lives. If you agree, please join me in disseminating the idea in the safety-critical software community. The defunct patent, which describes the idea, is a 38K ASCII text file that can be retrieved by anonymous FTP from:

Machine : sirius.itd.adelaide.edu.au [129.127.40.3] File : pub/compression/puzzlebox\_provpatent

My thanks go to all those who were involved last year,

Ross Williams, ross@spam.adelaide.edu.au



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mike Morton <mike@proponent.com> Tue, 28 Apr 92 10:45:47 HST

From the Honolulu Star-Bulletin's "Streetwise" column, 27 April 1992:

Time change leaves stoplights out of sync (By David Oshiro)

Here's a story on how the clever machines that run our lives are sometimes too clever.

Three weeks ago, most of the mainland switched to daylight savings time. Unbeknown to city transportation officials here, a microchip controlling traffic signals on Kalanianaole Highway contained a program written on the mainland that contained an automatic conversion to daylight-saving [sic] time. So, \*voila\*! On Monday, April 6, the timing for peak traffic hours kicked in an hour earlier, throwing signals off. Signals that were changing in 200-second cycles began to change in 185-second cycles.

It was only a 15-second difference, and it only lasted an hour, but that was enough to mess up morning rush-hour traffic [which is pretty bad on this highway].

City workers, however, were able to figure out the problem and fix it that day.

A city transportation official said that there was no easy way to test that chip in advance, to see it [sic] would have worked properly when the switch to daylight-saving time occurred.

Mike Morton <Mike\_Morton@Proponent.com>

### Is it getting too easy? (Spreadsheetology)

Robert Slade <rslade@sfu.ca> Mon, 27 Apr 1992 20:52:50 GMT

This past week I was at a Microsoft Technical Seminar (read "boasting session") and saw an interesting promotional piece. Although longer than a normal ad, I suspect it is planned to use the "playlet" for some kind of media presentation. The "plot" is that Microsoft's Excel spreadsheet is so easy to use, and has so many "labour saving" features that two dolts who have forgotten to put together their presentation are able to do so in a one minute elevator ride to "executive territory".

Other than stylistic aids, the primary function promoted is an "extension" function which will "forecast trends". With so much spreadsheet use being devoted to business plans and cash flow projections, the attraction of such a function is obvious.

However, the ad immediately triggered an alarm. The feature is introduced, in the ad, by the fact that the executive "wants to see ten percent growth". The original figure is \$1000, so the user fills in the next column as \$1100. No problem. Then the extension feature is brought into play, and I mentally follow along with the arithmetic. The next column should say \$1210. But the spreadsheet fills in \$1200. The fourth column should be \$1331, but instead is filled in as \$1300. Ah, to the numerate person, the reason is obvious: the function is not a geometric "ten percent growth" but an arithmetic adding of an additional hundred dollars each time.

To the numerate person, obvious. To the general public? How many of the "average" business computer users would even notice?

The RISK of this particular choice of "extension" algorithm might not be all that important. However, it points out the increasing addition of "aids" in computerized systems, and the need to note carefully the use that the using audience is likely to put those aids to. Business computer users, in my experience, tend to want to think in "percentage" figures (eg. annual growth). A simple "adding" function for forecasting will not give them the "correct" answer appropriate to their mental model.

Small though this RISK might be in this instance, we have seen this same principal at work in situations with much higher stakes.

### IEEE/CS Workshop on Ethical Standards for the Profession

<horning@src.dec.com> Mon, 27 Apr 92 17:47:20 -0700

This workshop is discussed at length in the April issue of COMPUTER, pp. 76-78. I don't recall seeing it on RISKS, although the general topic has certainly had its share of discussion and flame in the past.

Jim H.

## FBI and Mailing Lists

<MCULNAN@guvax.georgetown.edu> Mon, 27 Apr 1992 19:42 EDT

The 20 April 1992 issue of DM News, a direct marketing trade publication, reports that within the past two weeks, Metromail and Donnelly Marketing (two of the very largest mailing list companies) were approached by the FBI which is seeking mailing lists for use in investigations. Other mailing list firms also received feelers according to the story. "Neither of the identified firms would discuss details, but one source familiar with the effort said the FBI apparently is seeking access to a compiled consumer database for investigatory uses."

"The FBI agents showed 'detailed awareness' of the products they were seeking, and claimed to have already worked with several mailing list companies, according to the source."

Metromail, according to the article, has been supplying the FBI with its MetroNet address lookup service for two years. The FBI said that the database is used to confirm addresses of people the FBI needs to locate for an interview.

This marks the first time since the IRS tried to buy mailing lists in 1984 that a government agency has attempted to use mailing lists for enforcement purposes.

In a separate but related story in the April 24 issue of the Friday Report, a direct marketing newsletter, the RBOC's are teaming up with other firms to develop white page directories on CD-ROM. For example, US West has a joint venture with PhoneDisc USA of Marblehead, Ma. The article states that the company offers lists failing mailing list enhancements to law enforcement agencies. [NOTE: an enhanced list means the names and addresses were matched with a marketing database and additional demographic information was added to the list from the marketing database].

Mary Culnan, School of Business Administration, Georgetown University MCULNAN@GUVAX.GEORGETOWN.EDU

# Ke: Voice mail security (Dickson, <u>RISKS-13.44</u>)

Dan Wing <DWING@uh01.colorado.edu> 27 Apr 1992 21:25:31 -0600 (MDT)

>Are call loggers a problem when you give your password to a mail retreival>system form a hotel or an office. Is there a hacker market for this info?>Finally how prevelant is this problem in various parts of the world?

Many hotels detail your phone bill and include the phone numbers you called during your stay. How often does the hotel phone system capture your MCI/Sprint/AT&T calling-card number (which you touch-toned into the MCI, Sprint, or AT&T computer), too?

I can easily change the PIN on my voice-mail system; changing the PIN on my calling card requires a call to the long-distance carrier, and possibly a new card - something the long-distance carrier isn't going to want to do too often.

-Dan Wing, DWING@UH01.Colorado.EDU, WING\_D@UCOLMCC.BITNET Systems Programmer, University Hospital, Denver

# Ke: Tracking by cellular phone (Kush, <u>RISKS-13.44</u>)

<John\_Karabaic@NeXT.COM> Tue, 28 Apr 92 16:10:47 EDT

I had the same experience myself recently. But, in addition to instructions, it was also a telemarketing call by the local carrier! Since I use my cellular phone as a contact line for technical support and am always expecting calls (I subscribe to a nationwide switching service), I was rather angry that they used my time on the line like that. Especially since it was during a driving rainstorm while I was on the Interstate in the hills of northern Kentucky! I called \*611 and told the person on the line to get me off whatever list I was on to get this unnecessary greeting and unwanted telemarketing. I haven't been bothered since, but I don't know if my call got me off any "list".

John S. Karabaic, Systems Engineer, jkarab@NeXT.com, 513 792 5904 NeXT Computer, Inc.; 4434 Carver Woods Dr.; Cincinnati, OH 45242

# Ke: Tracking by Cellular Phone (Kush, <u>RISKS-13.44</u>)

<PHILLIP.D.BROWN#m#JR@gte.sprint.com> 28 Apr 92 15:29:00 UT

Not only \*could\* the cellular phone company track one's movement "all over the country" (although with great difficulty and expense using today's switches),

it is an active industry goal for the next generation of technology. "Call Delivery" -- making your phone ring when someone dials your number, regardless of your geographic location and serving carrier of the moment -- is an integral part of the standard being developed for interswitch communication (EIA/TIA IS-41). It is also seen as a key to making Personal Communication Networks (PCN) work.

What happened to you in Georgia is the result of a feature known as "autonomous registration", by which the serving switch instructs a mobile unit to register (i.e. transmit its identity information including mobile phone number and serial number) as soon as radio contact is established (as indicated on the mobile's handset display by the "service light" or "service bars"). When the system detected you were a roamer, it placed a call to your phone and played the recorded greeting for your edification (although I don't know BellSouth's policy, it is quite unlikely you were charged for this call).

Furthermore, Automatic Vehicle Location (AVL) services are also seen as highly desirable by a significant subgroup of wireless communication users (truckers and victims of car thieves come immediately to mind). There are companies that claim to be able to determine the position of a mobile unit in a cell site to within 100 feet using only the received 800 MHz radio signal, but the technology is unreliable and expensive. The more popular solution is to marry a Global Positioning System (GPS) receiver to a cellular phone or other wireless terminal, but this is both proprietary and also expensive.

As long as the user retains the ability to "disappear" by turning the phone off, I see the benefit as outweighing the risk in this form of network tracking. I squirm a lot more when I read about "beacons" placed in every car for automatic toll collection and vehicle monitoring, because these specialized systems exist solely for the purpose of tracking and accounting (NOTE: does anyone really expect there to be an "off" switch on such a device?). It's one thing to choose to be tracked, and quite another to have an "Eye in the Sky" checking up on you...

Phil Brown, Project Engineer, GTE Mobile Communications Internet address: phillip.d.brown#m#jr@gte.sprint.com

#### **COMPASS '92: Conference on Computer Assurance**

Laura Ippolito <ippolito@swe.ncsl.nist.gov> Fri, 24 Apr 92 09:20:30 EDT

First Announcement COMPASS '92: SEVENTH ANNUAL CONFERENCE ON COMPUTER ASSURANCE Systems Integrity, Software Safety, and Process Security

> June 15-18, 1992 Gaithersburg, Md.

National Institute of Standards and Technology Technology Administration U.S. Department of Commerce Department of Defense Approval: "In reviewing the Institute for Electrical and Electronics Engineer's Plans for COMPASS '92, the Assistant Secretary of Defense (Public Affairs) finds this event meets the standards for participation by DoD personnel under instruction 5410.20 and DoD Standards of Conduct Directive 5500.7. This finding does not constitute endorsement of attendance which must be determined by each DoD component."

CompassIEEE Aerospace and Electronic Systems SocietySponsorsIEEE National Capital Area Council

In cooperation with The British Computer Society

Conference Sponsors: ARINC Research Corporation, Computer Sciences Corporation Control Systems Analysis, Department of Defense, George Mason University Logicon, Inc., National Institute of Standards and Technology, Naval Research Laboratory, Naval Surface Warfare Center Research Triangle Institute, Systems Safety Society, TRW Systems Division

Program Committee:

Paul Ammann, George Mason University Greg Chisholm, Argonne National Laboratory John Dobson, University of Newcastle Upon Tyne Frank Houston, Food and Drug Administration William S. Junk, University of Idaho John Knight, University of Virginia D. Richard Kuhn, NIST John McDermid, University of York John McHugh, University of North Carolina Gerry Masson, Johns Hopkins University Reginald Meeson, Institute for Defense Analyses Andrew Moore, Naval Research Laboratory Matthew Morgenstern, Xerox Advanced Information Technology Jim Purtilo, University of Maryland Edgar H. Sibley, George Mason University Tony Zawilski, The Mitre Corporation

#### NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

A principal agency of the Department of Commerce's Technology Administration, NIST has as its mission to strengthen U.S. industry's competitiveness, advance science, and improve public health, safety, and the environment.

NIST conducts basic and applied research in the physical sciences and engineering, developing measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive research and development work on new advanced technologies.

NIST researchers work at the frontiers of science and technology in such areas as chemical science and technology, physics, materials science and engineering, electronics and electrical engineering, manufacturing engineering, computer systems, building technology and fire safety, and computing and applied mathematics.

#### INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

The Institute of Electrical and Electronics Engineers is the world's largest technical professional society. Founded in 1884 by a handful of practitioners of the new electrical engineering discipline, today's Institute is comprised of more than 320,000 members who conduct and participate in its activities in 147 countries. The men and women of the IEEE are the technical and scientific professionals making the revolutionary engineering advances which are reshaping our world today.

The technical objectives of the IEEE focus on advancing the theory and practice of electrical, electronics and computer engineering and computer science. To realize these objectives, the IEEE sponsors technical conferences, symposia and local meetings worldwide; publishes nearly 25% of the world's technical papers in electrical, electronics and computer engineering; and provides educational programs to keep its members' knowledge and expertise state-of-the-art. The purpose of all these activities is two fold: To enhance the quality of life for all peoples through improved public awareness of the influences and applications of its technologies; and, to advance the standing of the engineering profession and its members.

The IEEE, through its members, provides leadership in areas ranging from aerospace, computers and communications to biomedical technology, electric power and consumer electronics. For the latest research and innovations in the many diverse fields of electrical and electronics engineering, industry and individuals look to the IEEE.

> COMPASS '92 June 15-18, 1992 About the Conference

COMPASS is an acronym formed from COMPuter ASSurance, the subject of this conference, the seventh of a series that began with COMPASS '86. According to its charter, "The purpose of COMPASS is to advance the theory and practice of critical systems through the medium of scientific and engineering meetings and publications. The organization, under the IEEE, is dedicated to the study of critical systems, especially those using digital computers or other new technologies."

Critical systems are defined as systems whose failure could cause injury, loss of life, or significant property loss or damage. Such failures may be failures of commission, doing what should not be done, or of omission, not doing what should be done. Critical systems have failed in the past. Radiation therapy machines have killed cancer patients; industrial robots have killed workers; spacecraft have been destroyed; and, hackers have vandalized and/or stolen from information systems. The goal of COMPASS is to find and publicize ways to prevent unacceptable failures of critical systems.

COMPASS expresses the idea of "Pointing the Way" and of "encompassing" many technologies and technical disciplines. The logo, a variation of yin-yang overlaying a compass rose, symbolizes both of these ideas.

COMPASS '92 has adopted the slogan "Building The Right System, Right." This

expresses the need for the developers of critical systems to rigorously define the right requirements and ensure that they are satisfied, resulting in systems that function as intended.

The sponsors and organizers of COMPASS encourage you to participate in future COMPASS activities. Contact any member of the conference committee or the conference board for more information.

**Conference Committee** 

Board of Directors Chair: Dolores R. Wallace, NIST General Chair: Robert Ayers, ARINC Research Corporation Program Chair: Edgar H. Sibley, George Mason University Local Arrangements: Laura M. Ippolito, NIST Publications: Julie Langston, Computer Sciences Corporation Publicity: Paul Anderson, Space & Naval Warfare Systems Command Division Registration: Judy Bramlage, General Accounting Office Treasurer: Bonnie Danner, TRW Systems Division Tutorials: Michael Brown, Naval Surface Warfare Center

COMPASS '92, Monday, 15 June 1992

9:00 a.m. Tutorial 1: "Approaches to Developing Safety-Critical Software"

Stephen S. Cha, Charles H. Lavine, and Jeffery C. Thomas, Aerospace Corporation, El Segundo, Ca.

This tutorial surveys various software safety techniques proposed in literature or currently in practice. Following an introduction to software safety concepts, several industrial software development examples will be examined. The tutorial concludes with a discussion on formal methods and future research directions.

12:45 p.m. Lunch

2:00 p.m. Tutorial 2: "Interlocks-A Safety Engineering Tool"

Phil Sedgwick, Control Systems Analysis, Newport, RI

This tutorial introduces INTERLOCKS, a methodology and PC-based tool, that graphically describes and simulates the operation of computer system controls. INTERLOCKS, in use by the DoD, employs a graphic language familiar to hardware and software engineers-simple AND and OR logic. The result for safety engineers is an INTERLOCKS network that models and simulates the hardware, software, and operator events that are prerequisite to critical function initiation.

COMPASS '92, Tuesday, 16 June 1992

9:00 a.m. Opening Remarks, Conference General Chair: Robert Ayers, ARINC Research Corporation, Annapolis, MD.

9:15 a.m. The Technical Program, Program Committee Chair: Edgar H. Sibley, GMU, Fairfax, VA. 9:30 a.m. Keynote Speaker, John Rushby, SRI International, Menlo Park, CA. "What Really Goes Wrong, And What Might Fix It?"

11:00 a.m. Session 1 Verification Chair: Andrew Moore, Naval Research Laboratory, Washington, D.C.

"Using Z Specifications in Category Partition Testing", Nina Amla and Paul Ammann, George Mason University, Fairfax, VA.

"Verification of Numerical Programs Using Penelope/Ariel", Sanjiva Prasad, ORA Corporation, Ithaca, N.Y.

"Modular Verification of Ada Library Units", Carla Marceau and Wolfgang Polak, ORA Corporation, Ithaca, N.Y.

12:45 p.m. Lunch

2:00 p.m. Session 2 Security, Chair: Paul Ammann, George Mason University

"A Probabilistic Approach to Assurance of Database Design", Lucian Russell, Argonne National Laboratory, Argonne, Ill.

"Formal Security Specifications for Open Distributed Systems", Sead Muftik, DSV Dept., Stockholm University, Sweden and Univ. of Sarajevo, Yugoslavia

"A Formal Approach for Security Evaluation", John A. McDermid and Qi Shi, University of York, UK

4:00 p.m. Debate: Resolved: "Certain Safety-Critical Systems Should Not Be Computerized". Moderated by John Knight, University of VA

5:30 p.m. Close of Daytime Activities

7:00 p.m. Birds of a Feather Session, Marriott

COMPASS '92, Wednesday, 17 June 1992

9:00 a.m. Keynote Speaker, Ted Ralston, Ralston Research Associates, Tacoma, WA, "Preliminary Report on the International Study on Industrial Experience with Formal Methods"

10:30 a.m. Panel 1 Formal Methods in Industry

.., Naval Research Laboratory, Washington, D.C. Leo Beltracchi, United States Regulatory Commission, Washington, D.C.

12:45 p.m. Lunch

2:00 p.m. Session 3 Safety, Chair: M. Frank Houston, Food and Drug Admin., Rockville, Md.

"Efficient Response Time Bound Analysis of Real-Time Rule-Based Systems", Albert Mo Kim Cheng and Chia-Hung Chen, University of Houston, Houston, TX "The Use of Ada PDL as the Basis for Validating a System Specified by Control Flow Logic", Richard B. Mead, ARINC Research Corporation, Annapolis, MD.

One further paper to be selected

4:00 p.m. Panel 2 Software Safety and Economics, Chair: J. Bret Michael, George Mason University, Fairfax, VA.

Stephen Fortier, Intermetrics, McLean, VA.William S. Junk, University of IdahoEdward A. Addy, Logicon, Inc., Dahlgren, VA.John McHugh, University of North Carolina, Chapel Hill, N.C.

5:30 p.m. Close of Daytime Activities

6:30 p.m. Banquet with Dinner Speaker, Marriott

COMPASS '92, Thursday, 18 June 1992

9:00 a.m. Session 4 Processes, Chair: Reginald Meeson, IDA

"A Review of Computer Controlled Systems Safety and Quality Assurance Concerns for Acquisition Managers", John R. Friend, U.S. Navy, Polaris Missile Facility, Charleston, S.C.

"An Analysis of Selected Software Safety Standards", Dolores Wallace, D. Richard Kuhn, and Laura Ippolito, NIST, Gaithersburg, Md.

"A Process Representation Experiment Using MVP-L", Carol Diane Klinger, Melissa Neviaser, and Ann Marmor-Squires, TRW, Fairfax, Va.; Christopher M. Lott and H. Dieter Rombach, University of Maryland, College Park, Md.

11:00 a.m. Panel 3 Software in Trial - Liability and Other Legal Issues (A Dramatization)

Moderator: Michael S. Nash, Esq., IDA, Alexandria, VA

Jay T. Westermeier, Fenwick and West, Washington, D.C., For the Plaintiff To be selected, For the Defendant Richard L. Wexelblat, IDA, Alexandria, Va., As Expert Witness To be selected, Insurer To be selected, Harried Software Developer/Programmer

12:45 p.m. Lunch

2:00 p.m. Session 5 Software Safety Standards

"IEEE P-1228: Latest Status", Cindy Wright, DISA, Tysons Corner, Va.

"IEC65A, WG9 and WG10 -- System and Software Safety Standards for Programmable Electronic Systems", Victor Maggioli, DuPont, Newark, Del.

3:30 p.m. Awards and Closing Ceremony

4:00 p.m. Conference Closing

NIST is located in Gaithersburg, Md., approximately 25 miles northwest of Washington, D.C. The meeting will be held in the Green Auditorium of the Administration Building.

Social Functions: A banquet with a cash bar and banquet speaker will be held at the Gaithersburg Marriott on Wednesday, June 17.

Transportation: BWI Limo, 301/441-2345, offers commercial van service from Baltimore-Washington Airport to the Gaithersburg area. Call for reservations.

Airport Transfer Van Service, 301/948-4515, is available from Dulles International and Washington National Airports to Gaithersburg.

The Washington Metro has subway service to Gaithersburg. Metro can be boarded at Washington National Airport. Take a Yellow Line train marked "Mount Vernon Square" to Gallery Place and transfer to a Red Line train marked "Shady Grove" to Shady Grove. Service is every 6 to 15 minutes depending on the time of day. The time from National to Shady Grove is about 50 minutes. The Shady Grove station is approximately four miles from the Marriott Hotel.

Driving Instructions: From northbound I-270 take Exit 10, Rt. 117 West, Clopper Road. At the first light on Clopper Road, turn left on to the NIST grounds. From Southbound I-270 take Exit 11B, Route 124 West, Quince Orchard Road. At the second light turn left on to Clopper Road. At the first light on Clopper Road, turn right on to the NIST grounds. To reach the Administration Building, turn left after passing the guard office. Signs will direct you to visitor parking. Transportation will be provided to and from the Gaithersburg Marriott and NIST on Monday through Thursday.

Accommodations: Conference registration does not include your hotel reservation. A block of rooms has been reserved at the Gaithersburg Marriott Hotel, 620 Perry Parkway, Gaithersburg, Md. 20877. The hotel phone number is 301/977-8900. The special room rate is \$65 single or double. To register for a room, please use the enclosed hotel reservation form and send it directly to the hotel no later than June 1, 1992. After that date the rooms will be released for general sale at the prevailing rates of the hotel.

Registration Information Contact: Judy Bramlage, COMPASS '92 Registration 609 Orrin St., SE, Vienna, Va. 22180-4837, 202/512-6210, Fax: 202/512-6451

Technical Information Contact: Robert Ayers, ARINC Research Corporation, 2551 Riva Rd., Annapolis, Md. 21401, Phone: 410/266-4741 Fax: 410/266-4040

COMPASS '92 June 15-18, 1992 Conference Registration Card

Advance Registration (before June 1, 1992)

Conference Registration (includes 1 copy of proceedings)

\_\_\_\_ Proceedings Only

\_\_\_\_ Extra Proceedings \_\_\_\_\_ copies

\_\_\_\_ Tutorial #1 \_\_\_\_ Tutorial #2 Name Company Street Address Rm. No./Mail Code City, State, Zip Country **Business Telephone** IEEE Membership No. **Co-Sponsor Name** Total Amount US \$ \_\_\_\_ Check enclosed made payable to COMPASS '92. Form of Payment (Checks from outside USA should be written on a USA bank.) \_\_\_ MasterCard No.\_\_\_\_\_Exp.\_\_\_\_ \_\_\_\_ Visa No.\_\_\_\_\_Exp.\_\_\_\_ \_\_\_\_ Diners Club No.\_\_\_\_\_Exp.\_\_\_\_ \_\_\_ American Express No.\_\_\_\_\_Exp.\_\_\_\_ Authorized Signature Request for refunds after 1 Jun 1992 will be subject to a \$15 admin fee. **Registration:** Advance Registration (before June 1, 1992) Members Non-Members Students ----- -----Conference 250 315 100 Tutorial 50 70 50 Proceedings Only 20 30 20 \*\*\*\*\*\*\* On-Site Members Non-Members Students ----- -----Conference 300 375 100 70 90 Tutorial 50 Proceedings Only 20 30 20 Conference fee includes coffee breaks, lunches and social functions. Please place in an envelope and mail to: Judy Bramlage, COMPASS '92 Registration, 609 Orrin Street, SE, Vienna, Va. 22180-4837 COMPASS '92 June 15-18, 1992 Hotel Registration Card Marriott Hotel, 301/977-8900 Name Company Street Address Rm. No./Mail Code City, State, Zip Country **Business Telephone** Arrival Date

Departure Date Number of Persons

Rate: \$65 single or double (apply 12% tax to rate). All reservations must be received by June 1, 1992. All room reservations must be guaranteed by a one-night deposit. Deposit will guarantee first night availability, and will be credited to last night of reservation. Deposit refunded if request received 48 hours prior to arrival.

Form of \_\_\_\_ Check enclosed made payable to The Payment Gaithersburg Marriott \_\_\_\_ One night deposit enclosed \$\_\_\_\_\_ Guaranteed by\_\_\_\_\_ Exp.\_\_\_ Card #

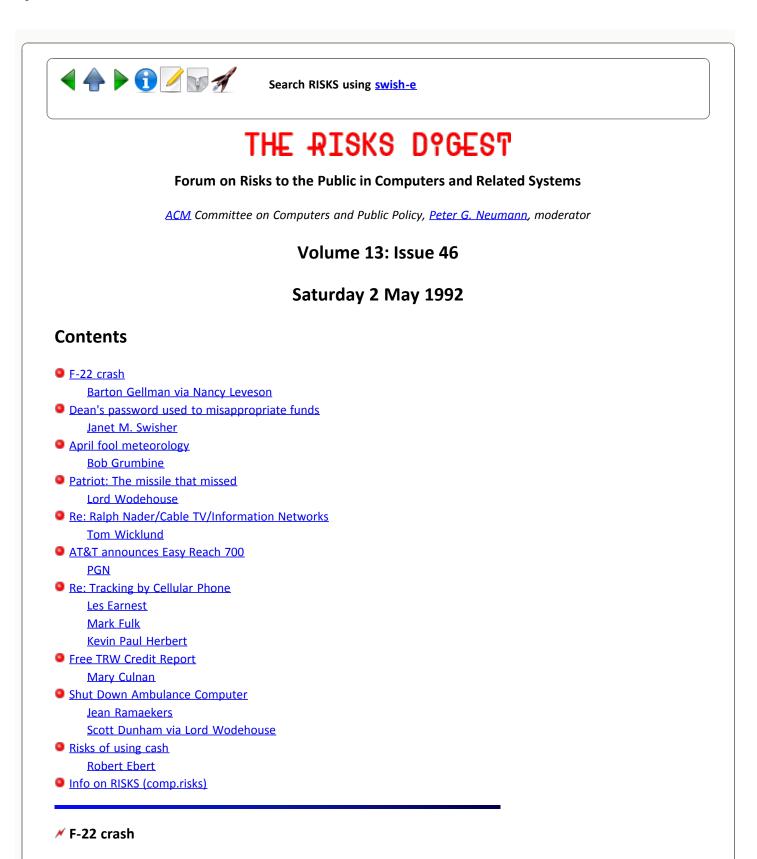
Authorized Signature\_\_\_\_\_

Please place in an envelope and mail to: The Gaithersburg Marriott, 620 Perry Parkway, Gaithersburg, Md. 20877



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<leveson@cs.UMD.EDU> Thu, 30 Apr 92 19:49:10 -0400

Here's a switch -- someone hoping the blame can be put on the computer.

Computer Problem Cited in Crash of F-22 Prototype by Barton Gellman

#### Washington Post, April 30, page A3

A computer software problem probably caused the weekend crash that destroyed the only flying prototype of the F-22 Advanced Tactical Fighter, the Air Force's top general said yesterday. Gen. Merrill A. "Tony" McPeak, Air Force chief of staff, told House Armed Services Committee panel that it will be good news for his top-priority weapon program if an investigative panel confirms what he calls his speculative explanation, because a software flaw is "relatively straightforward" to fix. [...]

Lockheed Corp. test pilot Tom Morganfeld, by this account, had just refilled his fuel tanks in preparation for a test of supersonic flight characteristics when he learned of a break in the telemetry link that sends performance data from the aircraft to the ground. The supersonic test was cancelled. Already airborne, the F-22 was too heavily laden to land safely, and so Morganfeld began a series of high-speed, low-altitude passes over the runway to burn excess fuel. On the second pass, Morganfeld lost control. Videotape of his last seconds in the air shows that he retracted the landing gear and ignited his afterburners at roughly the same time, and the plane's nose immediately began porpoising out of control. The F-22 crashed, burst into flame, and slid 8,000 feet -- well over a mile -- before stopping. Morganfeld escaped with minor injuries.

McPeak's theory of the crash said the combination of reduced drag from the retracted landing gear and increased power from the afterburners meant that the plane needed far more "slab authority" to control the aircraft. In other words, the F-22's control surfaces had to be raised and lowered more sharply. But on modern fly-by-wire aircraft, a pilot has no direct control of the physical movement of the flaps. Morganfeld's commands were interpreted by a computer- controlled servo-motor that continuously made thousands of calculations to adjust the controls, much as anti-lock brakes do on late model automobiles.

McPeak said he believed that "something in the logic of the fly-by-wire flight control system" failed to move the control surfaces far or fast enough to keep up with the pilot's commands. If an Air Force investigative panel bears out McPeak's hypothesis, according to experts, it will rule out far more serious problems with the aerodynamic stability of the plane during the critical "flight regine" of a landing approach. But McPeak acknowledged he does not yet have all the facts.

[This is Nancy Leveson, now at UMD, still on sabbatical from UCI. PGN]

#### ✓ Dean's password used to misappropriate funds

Janet M. Swisher <swisher@cs.utexas.edu> Thu, 30 Apr 92 13:05:13 -0500

The \_Austin American Stateman\_ and \_The Daily Texan\_ report that an employee of the University of Texas College of Engineering used a password belonging to a dean to misappropriate about \$16,200 from March 1991 to February 1992. The dean reportedly gave the employee the password, in violation of university policy. The employee resigned when confronted; no charges have yet been filed. Neither the dean nor the employee were identified to the press.

The funds were earmarked for travel fellowships for recruiting students from other universities; the employee awarded fellowships to UT students who were not eligible to receive them. UT police would not comment on whether the employee directly benefitted from the misappropriation. The improper payments were discovered accidentally when a student wrote to thank the associate dean of recruiting of the College of Engineering for the College's generosity. According the dean of the College, "That student didn't do anything wrong. He just came to the dean's office for assistance and he got some."

The employee had access to about \$300,000. The university is auditing its records to determine whether improper payments were made in prior periods. Legitimate awards were made from the same fund during the same period as the improper ones. The College of Engineering is tightening its security guidelines (no details given).

## April fool meteorology

<RMG3@psuvm.psu.edu> Thursday, 30 Apr 1992 16:45:22 EDT

In a recent Risks, we heard the story of a shotgun attack on a wind profiler. It develops that this was indeed an April Fool's joke. I've deleted the included text to save you bytes.

Bob Grumbine a.k.a. rmg3@grebyn.com

Newsgroups: sci.geo.meteorology From: skaggs@nsslsun.nssl.uoknor.edu (Gary Skaggs) Subject: Re: Hazardous Duty - Wind Profilers Organization: National Severe Storms Laboratory Date: Thu, 30 Apr 1992 13:56:08 GMT

>Excerpted from RISKS-LIST: RISKS-FORUM Digest Monday 27 April 1992 >Volume 13 : Issue 44

You got a second generation. Yes, you've been `APRIL FOOLED'!!!

This story appeared in a posting on OMNET by R.JUNE addressed to the noaa.erl.labs listing under the subject of weekly report.

The header reads thusly:

OCEANIC AND ATMOSPHERIC RESEARCH (OAR) WEEKLY REPORT FOR THE SECRETARY OF COMMERCE April 1, 1992

Besides the above story, other tongue in cheek submissions covered:

GLERL proposing to introduce the Chesapeake Bay blue crab into the Great Lakes to try to control the zebra mussel

An agreement with the Russian republic to rescue a data set of some 70 years of "potential greenhouse gases emitted by herds of Bovinas mermoska,

the Mongolian yak of central Asia."

A new ERL lab to Study the Effects of the Moon on the Earth. Jerry Brown announcing that if elected, he would create a NOAA/ERL lab called the Moon Environment Lab (MEL). (This one was REALLY good).

And a weather Modification Person of the Year Award to Saddam Hussein for taking weather mod out of the lab and into the atmosphere. He was cited for his willingness to "test scientific hypotheses through the examination of actual, not simulated or modelled, pollution events, and for initiating similar studies into the environmental effects of massive oil spills." Carl Sagan was the keynote speaker.

Sorry guys, you've been had ...

Gary Skaggs - WB5ULK skaggs@nssl.nssl.uoknor.edu DOC/NOAA/ERL/NSSL

[Also noted by Thomas Lapp <thomas%mvac23.uucp@udel.edu> and joe@montebello.soest.hawaii.edu (Joe Dellinger). PGN]

# Patriot: The missile that missed

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 29 Apr 92 12:31:00 BST

>From New Scientist 18 April 1992

(For other articles and comments, see RISKS-13.19, 13.32, 13.37)

Patriot: The missile that missed

While defending the performance of the Patriot missile last week, US Army officers reduced their estimates of how many Iraqi missiles the Patriot hit during the Gulf War. The army now believes that the Patriot successfully intercepted 24 missiles out of about 85 attempts. But it has "high confidence" in only 10 attempts.

Even as the Pentagon renewed its defence of the Patriot's record, new evidence cast additional doubt of its credibility. The congressional General Accounting Office revealed that the army's earlier estimates of the Patriot's success were wildly optimistic and were based on over=hopeful assumptions. For instance, if the army could not find an impact crater from a Scud warhead, it assumed that the Scud had been destroyed by a Patriot. Yet some army units on the scene never bothered to look for craters, says the GAO.

The Congressional Research Service, in a separate analysis of classified Pentagon data, concluded that most of the army's evidence was weak. Steven Hildreth of the CRS says that he is only convinced that one Patriot missile actually destroyed a Scud warhead.

During the Gulf War, President Bush announced to cheering crowds the Patriot had "intercepted" 41 out of 42 Scuds that it was fired at. General Robert

Drolet defended Bush's statement at last week's congressional hearing, saying that "intercepted" meant only that "a Patriot and a Scud passed each other in the sky".

The army has abandoned an investigation of Ted Postol, the professor at Massachusetts Institute of Technology, who has been among the Patriot's strongest critics (New Scientist 28th March). Postol had been accused of using classified data in an article he published that was critical of the missile's performance.

[It is very good news, if Ted Postol has been "cleared" and that no action will be taken against him. However the double speak "intercepted" by this article leaves me worried to say the least. Most people will believe the "successes" and thus expect great things to happen. When such over-sold systems fail, it is the scientists, who get the blame and the world starts to reject their achievements instead.]

Lord John - The Programming Peer <w0400@uk0x08.ggr.co.uk>

## Ke: Ralph Nader/Cable TV/Information Networks (<u>RISKS-13.44</u>)

Tom Wicklund <wicklund@intellistor.com> Tue, 28 Apr 92 16:36:09 MDT

> Summary: Your help is needed to secure an amendment to pending cable >television legislation. [...]

Hmm, is this in risks because of the risks of cable monopolies to consumers or because of the risk of Ralph Nader :-)

Unfortunately, this effort makes the false assumption that cable is a monopoly which needs to be regulated. Cable is in no way a monopoly, and the most effective way to control cable costs has been shown to be competition (rates are much lower in areas with 2 cable providers).

Mr. Nader's effort is, as expected from his political philosophy, an attempt to create a "consumer" group and force cable companies to promote it before their customers. These consumer groups would pay to have information sent to the consumer, but only "incremental cost" (e.g. the cost of an extra sheet of paper in your cable bill rather than having to pay their own postage).

These groups would lobby regulatory bodies and legislatures. This is apparently needed because regulatory bodies and legislatures are bought and paid for by the cable companies and so we need another organization to represent the citizen.

Of course, there's no reason why a consumer group can't be started by interested individuals and lobby the appropriate bodies -- many such groups exist today. This proposal is an attempt to subsidize such groups, not financially but by legislating reduced cost access to consumers.

This proposal reminds me of (Ralph Nader prompted) "public interest research groups" which have been started on many university campuses. When they started

their group at the University of Colorado, they promoted themselves as a consumer protection group, out to protect the average person (e.g. somebody stupid and gullible) from big business.

The problem is that rather than being funded like any other campus group, they proposed that all students be required to pay their fee (about \$2.00), then about 4 weeks after the start of the semester, well after tuition and fees had been paid, students could apply for a refund of the fee if they didn't want to pay it, finally receiving the refund several weeks after applying.

This method was desired because it provided the group the highest income (much higher than voluntary checkoffs). Of course, this method plays on the same apathy that they deplored when businesses tried something similar, but the hypocrisy wasn't noticed.

## AT&T announces Easy Reach 700

"Peter G. Neumann" <neumann@csl.sri.com> Sat, 2 May 92 13:21:46 PDT

Easy Reach 700 gives each subscribers a Unique Phone Number that remains unchanged for the lifetime of the subscription, and that indirects to wherever you want the call to be received. The caller does not know the receiving number or its location. The service begins on 15 June.

The subscriber can call the assigned 700-xxx-yyyy number, followed by a 4-digit PIN, then 1#, and then the number to which calls are to be routed. This can be done from ANY touch-tone phone (assuming compatible tones, which -- I have noticed -- is not always the case among clone-phones). The subscriber may choose to assign up to 19 different passwords to would-be callers, where the absence of a password blocks the call indirection.

Perhaps the system will be smart enough to detect systematic attacks such as a denial of service from a computer dialing your number, running through as many of the 10,000 possible PINs as necessary until the right one is found, and then forwarding your calls off into space. I suppose you would want automatic calling number identification to detect who is attacking. (I presume that it would indicate the original caller, and not the 700 number!)

Of course, following our discussions of schemes for tracking people (such as by cellular phone IDs), Easy Reach could be misused as an interesting database of your presumed whereabouts...

[Source: San Fran Chron, 29 Apr 1992, p.1]

## Ke: Tracking by Cellular Phone (Kush, <u>RISKS-13.44</u>)

Les Earnest <les@sail.stanford.edu> Fri, 1 May 92 16:08:14 -0700

I brought up the subject of cellular phone tracking in a short note to RISKS a year or so ago and learned that locating a given phone within a sector having

an area of a square mile or so is part of normal operations. All that is needed to track a given phone, whether or not it is in active use, is to save this information in the same way that billing data is saved.

Furthermore, a civil liberties lawyer with whom I discussed this issue believes that as things stand in the U.S., law enforment authorities may collect and use cellular phone tracking data without a court order, unlike tapping telephones. They would presumably need the cooperation of the cellular phone company in order to do this without a large investment, of course.

My opinion is that cellular tracking data should be accorded the same privacy protection as phone taps.

Les Earnest, 12769 Dianne Drive, Los Altos Hills, CA 94022415 941-3984Les@cs.Stanford.eduUUCP: . . . decwrl!cs.Stanford.edu!Les

## Ke: Tracking by Cellular Phone (Brown, <u>RISKS-13.45</u>)

Mark Fulk <fulk@cs.rochester.edu> Thu, 30 Apr 1992 17:20:50 GMT

Wouldn't it be cheaper, simpler, and less intrusive to use Skytel-like satellite pagers to notify people that they have a call? It would work like this:

You cellular phone contains a satellite paging receiver and antenna. When someone calls you, the switch has the paging satellites transmit your code and the connection id number all over the world. Your phone receives this info, recognizes that it is meant for this phone, puts the connection id into a buffer, and rings. If you pick up the phone and press the "answer" button, the phone transmits the connection id on a standard connection request frequency. The connection id encodes the origin of the call, so the switch at the recipient end can route the call. You can only be tracked when you answer the phone.

Since a pager id + connection id need only be about 80 bits long, one voice-grade satellite channel would be able to handle at least 800 calls per second. 125 voice grade channels would handle the entire U.S., if every individual had a cellular phone and received about 10 calls per day. (Note that the address of the pager would include the channel it listened to.)

Mark A. Fulk, Computer Science Department, University of Rochester, Rochester, NY 14627 fulk@cs.rochester.edu

## Re: Tracking by Cellular Phone (<u>RISKS-13.44</u>)

Kevin Paul Herbert <kph@cisco.com> Wed, 29 Apr 92 10:25:22 -0700

I was talking to my mother yesterday about a new device that she had installed in her car, required by the insurance company in order to insure the car at full value.

The device tracks the location of the car with sufficient resolution to even give driving speed. My father called up the service to "test it out", and they said where my mother was driving, as well as indicating that she was driving 30 in a 35...

If she did not get this locating device, her insurer would have only insured the car at up to 50% of the car's value.

She didn't know anything about how this data could be disclosed; she hadn't really thought about it.

The risks should be obvious.

Kevin

## Free TRW Credit Report

<MCULNAN@guvax.georgetown.edu> Wed, 29 Apr 1992 16:32 EDT

The RISKS of not checking one's credit report periodically, and especially before applying for a mortgage or other loan or a job have been well documented here and elsewhere.

According to USA Today, beginning April 30, you can get a free copy of your TRW credit report once a year by writing to:

TRW Consumer Assistance, P.O. Box 2350, Chatsworth, CA 91313-2350

Include all of the following in your letter: full name including middle initial and generation such as Jr, Sr, III etc., current address and ZIP code, all previous addresses and ZIPs for past five years, Social Security number, year of birth, spouse's first name. Also include a photocopy of a billing statement, utility bill, driver's license or other document that links your name with the address where the report should be mailed.

Mary Culnan, School of Business Administration, Georgetown University MCULNAN@GUVAX.GEORGETOWN.EDU

## Shut Down Ambulance Computer (<u>RISKS-13.38</u>,42,43)

Jean Ramaekers <jrama@ICSI.Berkeley.EDU> Wed, 22 Apr 92 09:33:38 PDT

in : The Sunday Telegraph (London), NO. 1, 622, April 19, 1992.

Fatal delays shut down ambulance computer

London Ambulance Service has shut down its new L1.5 million 999-call computer system and launched an inquiry into failures that have led to fatal delays in emergency services reaching patients. In a catalog of errors, the capital's ambulance service has admitted defeat and agreed not to implement a second phase of its computer system. But a spokesman said the delays were "not a system problem but human error". ...

Already the LAS was under severe pressure to resolve the sofware problems following the death of a 20-year-old diabetic, Kerrie Swannell, on February 7. Miss Swannell died cardiac arrest shortly before the ambulance arrived, an hour after it was called. It was said that calls had been lost when a visual display unit was turned off by mistake. ...

The computer-aided dispatch system (CAD) was introduced in January in south-west London, and despite the "lost 999 calls" was extended to the north-east of the capital on February 25. Mr Barber says the system crashed for 90 minutes every day for more than a week. ...

ICSI, 1947 Center Street, Berkeley Ca 94704-1105 phone (510) 642-4274 ext 147

## ✓ London Ambulance - comments

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 23 Apr 92 10:22:00 BST

I think that this whole area deserves airing. I hope some other readers in the UK are taking note! Lord John - The Programming Peer

23 Apr 92 09:45

From:'m21208@mwvm.mitre.org (Scott Dunham)'@RELAY (remote user)To:'w0400 <uk.co.ggr.uk0x08!w0400@mwunix.mitre.org>'@RELAY (remote user)Subject:London Ambulance (RISKS posting)

Date: Thursday, 23 Apr 1992 04:31:27 EDT From: m21208@mwvm.mitre.org (Scott Dunham) To: w0400 <uk.co.ggr.uk0x08!w0400@mwunix.mitre.org> Subject: London Ambulance (RISKS posting) Sender: M21208@mwvm.mitre.org

I used to be a public safety dispatcher in California (police, fire, AND ambulance), and all I can say about the current performance of LAS is that it would have gotten our entire staff sacked. Fifteen minutes to answer the phone at a safety critical service is completely, totally, absolutely unacceptable. Our standard was no more than 30 seconds, and generally by the second ring, with arrival of the ambulance at the scene often coming within 5 minutes of the first call. Even that is almost too slow, because you can lose heart attack victims in four minutes.

With eleven people on staff, even 30 calls on the same incident can be handled in a couple of minutes if the staff have a suitable display system available. Once the incident appears in the queue, subsequent calls are a matter of establishing the nature and location of the report (15-20 secs) satisfying yourself that it is indeed a repeat report, and letting the caller know that help is coming. (Another 10 secs, tops!) Except for absolutely GROSS mismanagement, I can see no reason for such horrible response times as are regularly reported for LAS. Such a service must be held to a performance standard commensurate with the seriousness of its task and assigned sufficient resources to meet that standard. I think it's safe to say that letting people die on the phone would not meet a reasonability check for ambulance service performance...

Scott Dunham (Internet: sdunham@mitre.org) MITRE/London 011-44-895-426572

#### Risks of using cash

<Robert\_Ebert.OsBU\_North@xerox.com> Mon, 27 Apr 1992 13:24:22 PDT

My wife works at a major department store. This weekend, she was called upon to translate for two non english speaking customers who had been detained for suspicion of passing counterfeit money.

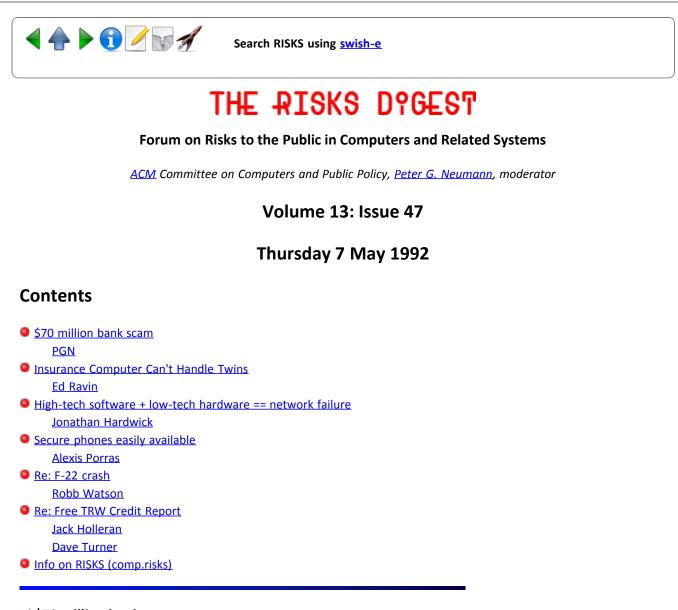
The two young men had made a small purchase (some socks) and paid with a US \$50 bill. Something about the bill (or perhaps the men) did not seem "right" to the clerk, and so the men were detained for more than an hour. The police were called, and their wallets were searched for more evidence of counterfeiting. [I don't know whether or not the search was made with permission.] The men spoke and acted innocently, and were confused and afraid by the proceedings.

It was determined that the bill in question was one of the new bills that are designed to \*prevent\* counterfeiting. Several other stores in the area were contacted in order to make this determination. The new bills have metallic threads woven into them, have a plastic "id stripe" in the paper that is visible when held up to the light, and have some design modifications. [My info from a "Nova" episode entitled "Making Money"]

I took a look at some new \$100 and \$50 bills at the local Credit Union, and they do look and feel different from the older bills. Additionally, the printing on the new bills looks rather poor, with green ink from the back "leaking" through to the face and much evidence of black ink being absorbed into the paper creating blur lines. [It's somewhat like the output from my DeskWriter on cheap paper!] It is, however, only marginally worse than the printing on a \$20. Perhaps the spotty printing helps to authenticate the bill-color copiers either do not have the problem or also blur the "colored threads".

aThe men were eventually freed, and advised to "use \$20 bills in the future." Some expired (but not forged) documents turned up as a result of the search were confiscated from one of the men. No attempt so far has been made to inform the rest of the store clerks of the different bills. It is disturbing to note that not much publicity has surrounded the issuing of the new bills. Neither the store personnel, the city police, nor the tellers at my bank knew anything about them, and if it hadn't been for the Nova episode neither would I.

While it may be risky to publicise anti-counterfeit measures, it seems more risky to hide the information from those who need to determine the legitimacy



# 🗡 \$70 million bank scam

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 7 May 92 18:33:41 PDT

The FBI is probing an electronic funds transfer scam that nearly cost First Interstate Bank of California \$70 million. A bogus request was made late last year to transfer the funds from `one or more accounts' at FIBofC to `one or more accounts' at other banks over the automated clearing house network. The request was made by computer tape, and apparently came with authorization forms and a signature -- possibly forged -- from a bank client. FIBofC apparently approved the transaction without validating its legitimacy, although this is not an uncommon practice. The bogus transaction was detected only because it caused an overdraft. This was the largest fraud attempt in the almost 20 years of the automated clearinghouse. The network handles transfers up to \$100 million, and carried about 1.7 billion transactions last year. [Source: American Banker, from the San Francisco Chronicle, 7 May 1992, p.C3]

## Insurance Computer Can't Handle Twins

Ed Ravin <eravin@panix.com> Tue, 5 May 92 21:27:06 EDT

LABOR PAINS, 1 YEAR LATER by Gail Collins (Excerpted from NY Newsday, 4 May 1992)

(Good morning. This is the Empire Blue Cross computer. If you have a problem with your insurance claim, press one to speak to a powerless employee. Press two if you would like to vent your grievance to a tape recorder.

(If you are not calling from a touch-tone phone, hang on until you get discouraged and give up. (Beep).)

OK, not the true tape recording. The true tape recording is less upfront. But it does yell: "I did not hear your response!" if it feels you are slow in pressing the appropriate button. Empire Blue Cross is the biggest health insurer in the state, and owner of one of New York's most infamous bureaucracies. Every day, innocent citizens fall into its maw.

"They'll never let you speak to a supervisor," said Michael Jacoby, another embattled customer. "They say: 'This is not a supervisor problem. ' "

I met Jacoby back in February, when he told me about his suspicion that Empire Blue Cross did not believe in the existence of twins.

At the time. Jacohy was in his 11th month of fighting over \$5,000 in doctors' fees connected to the birth of his twin daughters, Ashley and Brooke.

"I think they're discriminating against people with multiple births," he said. "My wife met somebody who had triplets. They were having the same problem. Basically, when the computer looks at the claims, it only looks at the birth date. It throws out the second child as a duplicate bill." Empire Blue Cross totally rejected this theory. "It must be a glitch. It's definitely not related to twins," said Michael Costa, a spokesman for the company. Meanwhile, the insurance company's lowly clerks were confirming Jacoby's suspicions. "It happens all the time." said one. taking time out from her duties in keeping Jacoby away from any person with authority to solve his problem.

Jacoby got no satisfaction, but lots of correspondence. And it did seem to buttress his theory about twins. There was a lot of documentation about payments for Ashley's treatment. But Brooke appeared to be a computer nonperson.

The twins were approaching their first birthday. The computer overpaid one of the pediatricians, while stonewalling the neonatologist who treated the girls when they were premies at North Shore University Hospital. "Our doctor was threatening to send the bill to a collection agency," said Jacoby. Actually. the neonatologist and her staff were understanding. It was the doctor's computer that was losing patience.

Jacoby sought help from the [New York] state Department of Insurance. "It will take a month," a woman at the state agency told him. A month later, there was no response from Empire Blue Cross.

"What do you do now?" Jacoby asked. "We send a second letter." "Then what do you do?" "We send a third letter." "Then what do you do?" "After the third letter, they have to respond. It's the law."

After the third letter, the agency did indeed get a response, from Linda Gummer, who holds the exalted title of Empire Blue Cross Executive Correspondent.

"Our claims processing system does have difficulty in distinguishing between one patient and another if both patients are covered by the same policy, have the same sex, birth date and are treated by the same doctor on the same date," she reported.

Translation: Our computer can't do twins.

"We shall see to it that our Customer Service area is alerted once again to this situation and that training... is reinforced."

The neonatologist got her money - just in time for the twins' first birthday.

"Now they're sending me benefits for using the North Adams Ambulance Service," Jacoby reported recently. "That's someplace in Massachusetts."

[Also noted by Joe Brennan <brennan@cunixf.cc.columbia.edu>.]

## Migh-tech software + low-tech hardware == network failure

<Jonathan\_Hardwick@GS69.SP.CS.CMU.EDU> Wed, 06 May 92 18:24:37 -0400

This network failure analysis was just posted to the facilities bboard here at CMU SCS. I guess it illustrates a potential risk of making a hard-copy log of all console messages...

Jonathan Hardwick, jch@cs.cmu.edu

\_\_\_\_\_

Date: Wed, 06 May 92 17:17:12 -0400 Subject: AFS tokens expiring Organization: School of Computer Science, Carnegie Mellon

This morning from about 11:30 am to 1:00 pm users who attempted to access afs files located on PEACH.SRV would get back an error saying that their token had expired. This anomaly was caused by the fact that PEACH's clock was an hour behind, so newly aquired tokens presented to its fileserver appeared to have a start time in the future and thus were rejected. The problem was fixed by manually resetting the time

The clock got so far behind due to the following series of events:

A process on PEACH was writing a file into AFS which was larger than the AFS cache on that machine. This caused the in-kernel AFS cache manager to continiously print the message :

" PEACH vmunix: afs: cache too small: flushing active file"

Since this message was being written to a 300 baud hardcopy console at a high interupt level, it was causing significant delays to the rest of the system. One of the results of these delays was that clock interupts were lost, and another was that 'ntpd' was not given a chance to run and fix the time skew. By the time the process acausing the problem finished the time skew was too large for ntpd to make adjustements, thus manual intervention was required.

# ✓ Secure phones easily available

<ap@wnb3b2.att.com> Thu, 7 May 92 14:15 CDT

Well, it didn't take very long for the FBI's proposed new rules to be defeated by the marketplace... this is an excerpt from an AT&T newsbrief (quoting Reuters).

\*\*\* SECURE PHONE -- AT&T said it introduced a new line of secure telephone equipment intended for business use. The model 4100, the first product in the 4000 Series, is designed to protect domestic and international voice and data communications. The company said that in the past, a secure telephone meant sacrificing voice quality, and the model 4100 offers voice quality comparable to a non-secure phone. [Reuters, 5/6]

Alexis Porras, a.porras@att.com

# 🗡 Re: F-22 crash

Robert A. Watson - SunNet Manager Engineering. <Robb.Watson@eng.sun.com> Mon, 4 May 92 13:45:56 PDT

I saw a 6 or 7 second video clip of this crash on a TV news program early last week. This video was shot from around the threshold of the runway, look towards the rear of the aircraft as it (fortunately :-)) flew away from the camera. During this sequence you could see massive (subjective term) up and down movements of the all-moving horizontal tail surfaces as the pilot (or the computer?) tried to stabilise the aircraft. As far as I can recall the gear was up for the duration of this sequence.

Odd that the software should be seen as a possible cause of the crash, when it would seem (to me) that this is exactly the sort of situation where it should have helped, assisting the pilot in managing a heavy aircraft flying close to the ground by compensating for extreme pilot input... humm, more or less what the General said, but with a different emphasis!

I though most aircraft could dump/vent excess fuel, you don't have to be at low altitude to do this, do you?

Robb

## Ke: Free TRW Credit Report (Culnan, <u>RISKS-13.46</u>)

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL> Wed, 6 May 92 09:09 EDT

Wow! What an advertising coup. If you weren't on their database before the request, you certainly are now.

And you can provide them with your SSN (without a privacy statement!), and your spouses' name, and a copy of a current bill ... from anyone will get you your record.

And if the business that sent the bill isn't a TRW customer, I would project that they will receive some advertising literature on how TRW can help their business.

Some other risks --- someone could set up a "favored" credit rating by using a false address on a short street. e.g.-My street has 7 houses {1-6, 8}; I could invent 7 (in the range) or 11 (a typo for my # 1); I could send a false bill to myself; and I could use a SSN. This could allow me to establish a potentially false credit information base for fraudulent use.

## Ke: Free TRW credit Report

<ptsfa!dmturne@pacbell.com> Mon, 4 May 92 12:56:30 PDT

The RISK of blindly mailing private information to an address posted in a computer bulletin board should be obvious.

Dave Turner (510) 823-2001 {att,bellcore,sun,ames,decwrl}!pacbell!dmturne

Report problems with the web pages to the maintainer



Fernando Pereira <pereira@mbeya.research.att.com> Fri, 8 May 92 20:30:35 EDT

The Associated Press reports today from Crosby, N.D, that farmer Harlan Johnson who was expecting a \$31 check from the U.S. Agricultural Stabilization and Conservation Service received instead one for \$4,038,277.04. Dale Ihry, head of the agency's office in North Dakota said that their computer program occasionally picks that particular amount and prints it out on something, although this is the first time that it was printed on a check. The farmer returned the check the day after.

It's wonderful how the agency seems to accept the bug as an act of God. Looks to me instead like an act of off-by-one indexing into an inappropriate memory location...

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave, PO Box 636 Murray Hill, NJ 07974-0636, pereira@research.att.com

## Moving time started even earlier this year

"David J. Fiander" <davidf@golem.uucp> Sat, 9 May 1992 08:50:58 -0400

The following excerpt is taken from shortwave radio magazine \_Monitoring Times\_, May 1992 issue:

Does anyone have the correct time?

When subscriber Fred Latus ... came in at 5 a.m. to "open up" station WKTV-TV ... he felt something was amiss with the clock - an ESE NBS Master Clock receiver, locked to WWV's time signal. Not having time to check it, however, it wasn't until a second engineer arrived and asked why the digital clock was one hour fast, that it hit him. [...]

"Having had problems with our receiver and antenna the past few months, we thought it could be our problem. By eight a.m. I had reset the system twice and it still was in error."

"About 9:15 a.m. I finally got an engineer at WWV, just coming on duty at 7 a.m. MST." ... Keeping Fred on the phone while he checked the computer, he came back to report that, sure enough, a "3" had been entered instead of a "4" for the month starting Daylight Savings Time.

... The United States had been on Daylight Savings Time for about nine and a half hours a month early and only half a dozen people caught it!

Since the rule for determining the start of daylight savings time is so simple (in the US), why isn't there an easy way to describe the rule, rather than punching in a date every year (as would seem to be the case).

[... It is not trivial, however, because any program older than a few years will get the shift wrong! The switchover used to occur on the LAST Sunday in April, and now is on the FIRST Sunday. PGN]

## C-17 software problems

Mark Seecof <marks@capnet.latimes.com> Fri, 8 May 92 15:34:32 -0700

In a story by Ralph Vartabedian on page D-12, Friday, 8 May '92, the Los Angeles Times reported [brutally condensed by M. Seecof]:

GAO Says C-17 is Riddled With Computer Problems

The McDonnell Douglas C-17 cargo jet is plagued with serious computer hardware and software problems, resulting in part from shortcuts taken by the company ... according to a General Accounting Office report obtained Thursday.

The GAO report is the first public finding that the C-17 has serious computerization problems, though Air Force documents have hinted before that the computer system lacks adequate capacity and that its development has fallen behind schedule.

The GAO report asserts that the software ... has been ``a major problem..." It found that the Air Force wrongly assumed that the software portion of the program would be low-risk and ``did little to manage its development or oversee the contractor's performance."

The C-17 is the most software-intensive transport aircraft ever developed. The report said the aircraft has 19 different on-board computers, using 80 microprocessors and functioning in six different computer languages.

The GAO found that the Air Force ``made a number of mistakes," including underestimating the size and complexity of the task, waiving many Pentagon standards for software development and awarding a contract to McDonnell that gave the firm control over software.

McDonnell officials declined to comment on the GAO report. But the report notes that both the Air Force and McDonnell concurred with its findings.

END OF STORY. Mark Seecof asks: has anyone seen the report itself? I'd like to know in what way it was a mistake to give McDonnell-Douglas control over software development for a plane it was building?

# ✓ Composite Health Care System at Walter Reed Hospital

"Peter G. Neumann" <neumann@csl.sri.com> Sun, 10 May 92 14:07:57 PDT

Walter Reed Army Medical Center has a \$1.6 billion computer system intended to streamline health care in the U.S. military. It has gotten low marks from WRAMC personnel, who attribute bungling of prescriptions, patient-care records, and doctors' orders to software glitches. One doctor said that use of the system increased his workload by up to two hours per day.

The system had been used for two years for admissions and general record-keeping, but the problems began when laboratory and pharmacy orders were incorporated. One doctor stated that his name was linked with patients he had never seen. Another noted that access to narcotics was not secure.

About half of the 625 doctors do not use the system for in-patient lab orders, although most do use it for radiology and pharmacy orders.

[Source: An article by Christine Spolar in the Washington Post, appearing in The Times-Picayune, New Orleans, 2 Feb 1992, p.A-22, and submitted (somewhat belatedly) to RISKS by Sevilla Finley.]

[I missed this one altogether at the time. A review was held later, in March. I hope a reader can provide an update -- including someone from SAIC in San Diego, which designed the system. PGN]

#### A Newspaper Risk?

<horning@src.dec.com> Fri, 08 May 92 14:28:56 -0700

----- Forwarded Message

From: axd7104@acfcluster.nyu.edu (Aaron Dickey) Newsgroups: alt.folklore.computers,alt.folklore.urban Subject: Microsoft advocates killing of Jews Date: 29 Apr 92 23:24:20 GMT

Hey everyone!! Did you know that Microsoft is advocating the killing of Jews in New York City? I sure didn't! But it's true! I read it in the paper!

Get ready for a whopper. Once again the news media proves that it doesn't know the first thing about computers. The entire story, retransmitted without permission, is below, as it appeared in today's New York Post.

For those who don't know, the Post is a tabloid paper, where the entire front page is one huge headline. So, screaming out at millions of New Yorkers this morning was the headline, "PROGRAM OF HATE". Above the headline is a photo of one of those old PC green-screen displays, with "NYC" = <skull> <Star of David>

## 🗡 DATATAG

<Brian.Randell@newcastle.ac.uk> Fri, 8 May 1992 11:31:37 +0100

The following article appeared in The Independent (do I have to keep on explaining to RISKs readers that this is one of the "quality" national newspapers here in the UK?) and is reprinted in its entirety without permission.

Typically of such articles, there is only a discussion of the advantageous uses, rather than the possible risky misuses of the device described. I smiled wryly at the claim that "We haven't thought of a question yet which we could not answer in our favour" - perhaps they should have asked RISKS! :-)

Incidentally, I wonder how this device relates to the similar devices that are being being advocated, and perhaps already used, for tagging pet dogs by implanting a the device under the skin. (This idea was a hot topic a year or so here in Britain, after some horrific incidents involving pit bull terriers mauling and indeed killing children.) Brian Randell

-----

FIRM OFFERS "FOOLPROOF" CAR SECURITY SYSTEM, by John Arlidge

A "FOOLPROOF" car security system could be available this year. Datatag, which uses hidden microchips to identify vehicle owners, was launched for motor cycles yesterday and car owners could be using it this summer.

Police, ministers and insurers have praised the system, the first of its kind offered to road users.

Hugh Chamberlain, managing director of Chamberlain Engineering, who will head a company to be formed next week which will market Datatag for cars, said he thought the new system was foolproof "It is a watershed. We haven't thought of a question yet which we could not answer in our favour."

Motorists would install microchips - about the size of a 5p coin - anywhere in their vehicles. Each chip would have a unique, pre-programmed code number which could be "read" using a special electro-magnetic "gun" which will be distributed to police forces around the country.

The codes would be logged on a secure police computer with engine and chassis numbers and the owner's name. Motorists could install as many microchips as they wanted. Five chips and registration would cost about (pounds) 40 - less than half the price of an alarm.

Hologram stencils which could not be removed or window etchings would warn potential thieves that the vehicle had been tagged.

An estimated 2,500 motorcyclists are already using the system to prevent theft and the sale of bikes and bike parts. Two hundred motorcyclists a day are tagging their machines.

Commander George Ness, of the Metropolitan Police stolen vehicles squad, said the system was very good. "It will help police re-cover stolen property and will have a considerable deterrent effect on the thief." But he added: "It is early days. It is the front edge of technology" The new system would not prevent joyriders stealing cars.

Mr Chamberlain, who predicted do-it-yourself Datatag kits would be on sale by July, said microchips hidden in inaccessible places - inside seats or down tubes - would mean that even if they could locate the chips, thieves could not remove them without damaging the car, reducing its value.

Thieves could never be sure that they had removed all the chips and if they tried to sell a car, prospective buyers could check if it was stolen.

Michael Jack, Minister of State at the Home Office, speaking at the launch of Datatag yesterday praised it as "part of industry's efforts to find the solutions" to auto crime.

>From this summer Norwich Union, which insures more of Britain's 22 million

vehicles than any other company, will send leaflets to motorcycle policy holders informing them of the advantages of Datatag.

Vehicles are stolen at a higher rate in Britain than any other European country. More than 580,000 vehicles were stolen in England and Wales last year and more than 913,000 thefts from vehicles were recorded. Auto crime accounts for almost a third of all recorded crime.

Experts believe Datatag could be used to "owner code" almost any item - from videos to antiques.

## **Ke:** \$70 million bank scam (<u>RISKS-13.47</u>)

<tep@tots.logicon.com> Fri, 8 May 92 10:00:47 PDT

It appears that the attempted \$70 million bank scam may be affecting bank customers. All of our employees received a phone mail message from our corporate payroll department warning us that "due to bank difficulties", our bank (First Interstate Bank of California) would be slow in processing automatic payroll deposits; we could expect that deposits which normally are made to accounts Thursday night (May 7) would not be made until Friday night at the earliest, but would not be made any later than Saturday night. No other reason was given.

Since this is the first delay in the nine years I have been here, I find is \*interesting\* that this coincides with FIBoC other difficulties.

(It could be due to difficulties in Los Angeles, but as the bank corporate offices are nowhere near the riot area, I consider that a remote possibility.)

Tom E. Perrine (tep), tep@Logicon.COM

## Ke: April Fools' Meteorology

Bear Giles <bear@tigger.cs.colorado.edu> Fri, 8 May 1992 18:37:10 -0600

I just wanted to let you know that I did \_not\_ know the report of hunters vandalizing a profile was bogus. The information posted on our bulletin board had no originating information on it, but \_did\_ have a "approved by" stamp in the corner indicating the office of the Director of the Boulder Labs had reviewed it.

Furthermore, none of the people I discussed this with knew it was a joke either. At our site/floor it appeared a legitimate news report. It didn't even seem unreasonable, knowing some of the situations others have reported. (The hippies who sued the National Park Service after being struck by lightning -- while holding a metal railing on a stony outcrop in a thunderstorm -- comes to mind). I'll protest this on Monday. I have no problem with April Fool's jokes (as the original article was clearly intended) which can be identified as April Fool's jokes, but posting an April Fool's joke a month later with no indication of its nature is a different matter. At least the newspaper clippings on my door, e.g. "Mom carried 12 miles by Tornado!" are clearly from the \_Weekly World News\_!

Bear Giles bear@fsl.noaa.gov

Apologies for any inconvenience my misinterpretation of the article may have caused.

## Ke: Free TRW Credit Report (Turner, <u>RISKS-13.47</u>)

## <MCULNAN@guvax.georgetown.edu> Fri, 8 May 1992 08:10 EDT

Re Dave Turner's accurate assessment of the RISK of blindly mailing private information to an address posted in a computer bulletin board, you may verify the earlier posting from USA Today (Money section, P. 1B, April 27 1992, Final Edition).

Second, people have expressed concerns about TRW building a database from the information people supply when they request their credit rpt. The research I have done on direct marketing over the past two years suggests that TRW won't learn \*anything\* new from us if people do supply all the info they ask for because TRW already has this AND MORE.

TRW maintains an extensive marketing database on individuals from which it sells mailing lists. The source of this information includes public records (drivers license, deeds, USPS change of address information), credit reports, and information it has purchased from mail order companies.

Names and addresses may be selected based on such factors as exact age, height, weight or whether or not you wear glasses (from drivers license records), information about a home mortgage (amount, type), recording date and whether or not the transaction was a purchase or a refinance (deed/tax assessor records), whether you are a "new mover," the distance of your move and whether it is local, regional or out-of-state as well as the date (USPS change of address information), whether you are a credit shopper, an active credit shopper, your purchasing power (credit report) and whether you shop by direct mail, are a multi-category buyer, recent purchase date, and category of purchases (e.g. collectors, crafts, high tech, sports, etc. etc) (information purchased from unspecified third parties).

TRW is not the only company in this business. There are a number of large direct marketing firms which sell similar types of lists.

We would all be able to exert much more control over the secondary use of our personal information if public records came with a check-off box, allowing each person to decided whether or not he/she wanted to received solicitations because they bought a house or car, moved and changed their address, or got a drivers license. Currently you can only ask these companies not to resell your

name by writing to them directly or by signing up for the DMA's Mail Preference Service. This will keep your name off of mailing lists, but it's not clear if it stops your name from moving around for those who are concerned about this.

Mary Culnan, School of Business Administration, Georgetown University MCULNAN @ GUVAX.GEORGETOWN.EDU

## Risk of direct deposit

Stuart Bell <stu@mwvm.mitre.org> Friday, 8 May 1992 09:23:17 EDT

I, and my brother, use direct deposit to avoid the risk of lost, stolen or forgotten pay checks. Nice deal. Last week, the company apparently decided he was paid a bonus check in error. Several days after the check had been electronically deposited to his account - and he had been notified of the amount - they reversed the deposit and withdrew the amount. He was not notified the bonus was withdrawn, nor was he notified (until the overdrafts arrived) that his account was reversed.

He is disputing the reversal of the decision to pay the bonus - and the company and bank are cooperating in notifying the folks who got the bounced checks and reversing the associated charges - but, it seems quite a risk to know that if you authorize direct deposit, you are also authorizing an implicit direct withdrawal.

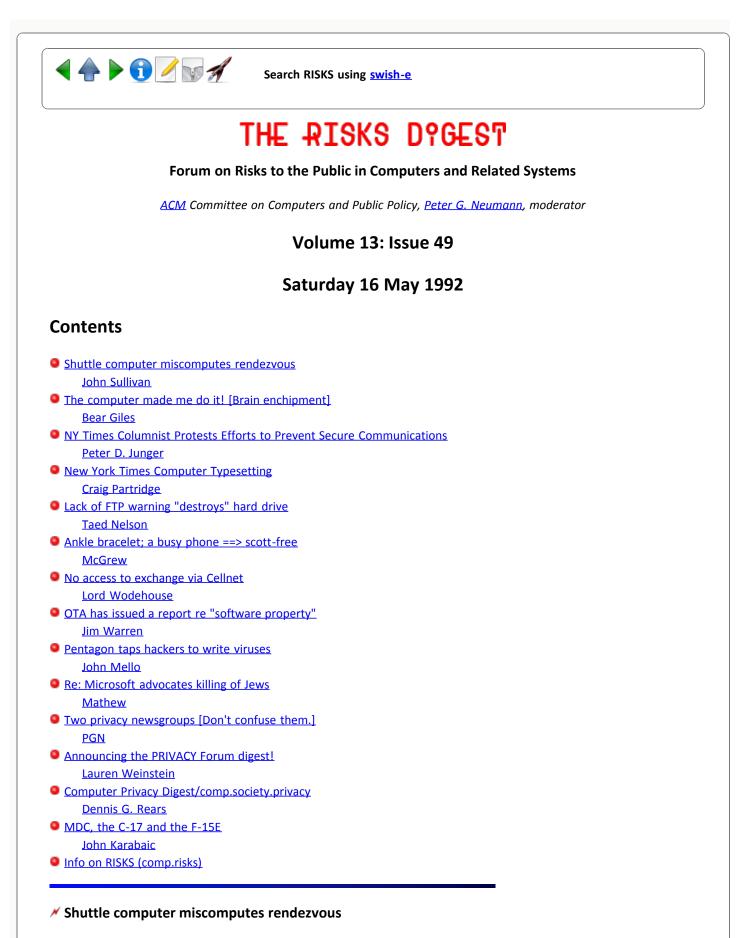
Maybe I'll ask to be paid in cash! The company is a large one and is in no financial difficultly so the problem was human or computer-to-computer and just left the poor worker out of the loop. /Stu Bell

MS=NASA (713) 333-0906 STU@MWVM.MITRE.ORG



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<sullivan@geom.umn.edu> Thu, 14 May 92 16:32:19 CDT Buried in a lead article ("from News Services") about the space shuttle in this morning's (Minneapolis) Star Tribune is the sentence:

The spacewalk was [...] delayed for 1 1/2 hours because Endeavour's on-board computer made a mistake in plotting the route needed to rendezvous with the satellite.

I hope someone will have more information on this.

-John Sullivan@Geom.UMN.Edu

# \* The computer made me do it! [Brain enchipment]

Bear Giles <bear@tigger.cs.colorado.edu> Fri, 15 May 1992 11:46:17 -0600

\_Rocky Mountain News\_, 15 May 1992, page 211

Computer Chip Get Blame

A woman who went on trial Wednesday in the shooting of three people at a Denver homeless shelter three years ago blamed the rampage on a computer chip she said her ex-husband planted in her brain. Juanita Whitaker, 42, pleaded innocent by reason of insanity in the Dec. 7, 1988, attack at the Brandon Center for homeless and battered women. One victim, a maid at the center, died in the attack.

Bear Giles, bear@fsl.noaa.gov

# MY Times Columnist Protests Efforts to Prevent Secure Communications

Peter D. Junger <junger@samsara.law.cwru.edu> Thu, 14 May 92 13:04:41 EDT

William Safire's column in the New York Times for May 11, 1992 (Page A15, Column 1) contains a sharp attack upon the Bush Administration's efforts to prevent the use of technology designed to allow secure communications. The essay is called: "Foiling the Compu-Tappers".

Here are some quotes:

[...] You might think, with foreign economic spies intercepting our global data transmissions, faxes and phone calls, the Bush Justice Department and National Security Agency would be helping American businesses defend communications from prying eyes and ears of overseas competitors eager to steal our scientific advantage.

The opposite is the case. In a policy blunder ranking with the adoption of the Smoot-Hawley tariff as depression loomed, the Bush Administration sent F.B.I. Director William Sessions to Congress to argue for a weakening of the devices U.S. citizens use to encode and keep confidential the information our

competition would love to see. [...]

This is a classic case of falling off the pace of change. In the name of law enforcement, we are making ourselves technologically vulnerable to international criminality. To preserve the huge investment in our old eavesdropping facilities, we are abandoning the field to modern organized crime.

Does anyone seriously think that state terrorism cannot afford the best encryption and penetration software, or that drug cartels cannot buy the latest encryption devices for their money movements? [...]

The trouble with both our Federal law enforcement and intelligence services is that they have become hooked on yesterday's technology. Electronic surveillance for cops and satellite photography for spooks have become central to their lives; their reaction to the inexorable improvement in encryption is to say to the world of science: slow down.

It won't. In trying to sweep back the tide of change, King Canute-style, the F.B.I. is the front for the intelligence community, which hates to be forced to go back to the difficult days of running human spies. The N.S.A. (No Such Agency) is obsolescent because its expensive eavesdropping is an offensive weapon in the coming age of digital defense. [...]

Mr. Bush is on the wrong side of this issue (and Ross Perot will take him apart on it in debate) because his mindset is toward old-fashioned spookery and against personal privacy.

In the end, that's what this futile scramble to stop the scrambling will come down to: not to stop the march of progress, not to take tools from counterspies, but to preserve business and personal privacy.

The coming Information Age threatens to be intrusive; the individual will be watched, examined, crowded. At the same time, to the happy tune of "I got algorithm," the computer-telephone complex brings us defenses against its own intrusion.

Peter D. Junger, Case Western Reserve University Law School, Cleveland, OH Internet: JUNGER@SAMSARA.LAW.CWRU.Edu -- Bitnet: JUNGER@CWRU

## New York Times Computer Typesetting

Craig Partridge <craig@aland.bbn.com> Tue, 12 May 92 12:34:26 -0700

Has anyone else noticed that the New York Times (at least the west coast edition) seems to have lots of trouble with computer typesetting?

Yesterday they had a notice on the front page that due to computer problems, some articles were not complete. The issue also had a lot of articles with headlines in the wrong fonts. It looked rather like someone had put the paper together by cut and paste.

Today, the pull-out quotes in Science Times were scrambled so that the article on jury behavior had pull-out quotes from the article on crystals in the human brain. Made for an amusing, if accidental, editorial.

Craig Partridge E-mail: craig@aland.bbn.com or craig@bbn.com

## ✓ Lack of FTP warning "destroys" hard drive

Taed Nelson <nelson@berlioz.nsc.com> Fri, 15 May 92 16:50:40 PDT

About a year back, a co-worker asked me how to re-partition his hard drive. I told him that this was a silly idea, considering that he had lots of space and the partitions didn't get into anyone's way. He just wanted to do it because it was "better".

Anyway, after explaining that he would have to save all of the old data some place (and suggesting that he not use millions of floppies, but instead FTP it up to our Unix system), he went away.

About an hour later, he came back asking for PKzipFix. I asked him why, and he told me that PKunzip was complaining that he had a bad ZIP file. I went over to his desk, and after about 15 minutes of questioning, I realized what had happened.

He had PKzip-ed each of his partitions and FTP-ed them up to the system. Unfortunately, he did not specify BINARY mode, and so it only transferred ASCII characters and converted CRLFs to LFs. Since he had reformatted his drive, all of that data was lost...

The RISK was that FTP had no warning message of the following sort:

WARNING: Non-ASCII characters found while in ASCII mode. I suppose that some further argument could be made that BINARY mode should be the default (instead of the data-modifying ASCII mode)...

## Ankle bracelet; a busy phone ==> scott-free

<mcgrew@cs.rutgers.edu> Wed, 13 May 92 15:08:32 EDT

`Busy signal' aided an `anklet' escapee (Newark "Star Ledger", 13 May 1992, By Robert Schwaneberg)

A Paterson man charged with committing a murder while he should have been under house arrest was able to beat the electronic system monitoring his where-abouts because a computer got a busy signal - and never called back. That was the explanation members of the Senate Law and Public Safety Committee were given yesterday as to how Tony Palmer was able to remove the rivets from his electronic anklet and have the tampering go undetected for four months. In fact, the computer at the Corrections Department headquarters in Trenton detected the tampering on Dec. 16 and printed the information out, according to Steven Adams, supervisor of the electronic monitoring-home confinement program. But when the computer tried to relay the information to computer monitors sitting just a few feet away, it got "a busy signal," Adams said. "It did not call back," he added.

As a result, senior parole officers manning the monitors 24 hours a day, seven days a week never knew what the computer knew - that Palmer had tampered with his anklet and that the computerized phone calls assuring that he was at home were worthless.

Sen. Louis Kosco (R-Bergen), the committee chairman, was incredulous at first. "I don't accept the answers that I've gotten," Kosco said. "How could this have happened for four months - time after time after time?" Corrections Commissioner William Fauver and other staffers explained that once the computer detected the tampering, any additional tampering would not set off new warnings. Adams explained that the device remained in "tamper status" until it was reset. When Kosco realized the implications of that, he was even more appalled. "If someone could get away with it one time, then he had carte blanche," Kosco said. "If you can get away with it one time, you're free."

"That's what happened in the Palmer case," conceded Loretta O'Sullivan, the Corrections Department's egislative liaison, "but it will not happen again."

Adams said parole officers in Trenton now scrutinize the computer printouts for information about tampering, disconnected phone service or an inmate on home detention failing to answer when called. Any such incident would trigger an immediate visit from a parole officer, he said.

Other staffers said that when parole officers visit home jail inmates once a week, they no longer rely on a visual inspection of their anklets but insert them into a verifier, which would show if the anklets are in "tamper" mode. By the end of the month, Adams added, the state should begin receiving new anklets that attach with interlocking metal bands rather than rivets. Adams, displaying one of the new anklets, said, "The only way this can be removed is by cutting it off."

Sen. Bradford Smith (R-Burlington) said a "major fault" of the current system is that even when an anklet is in tamper mode, the inmate can still use it to check in when the computer calls to see if he is home. Smith said that if the device has been tampered with, that should trigger an alarm each time a call is made to the inmate. "The technology has got to be up-graded in some fashion," Smith said. "This is just not acceptable." The anklets and monitoring equipment were manufactured by Digital Products of Florida, which did not have a representative at yesterday's committee meeting at Corrections Department headquarters. "I think we ought to look at some other systems and see what other companies are doing," Smith said.

Despite their apparent distress at the technical limitations of the system, the lawmakers said the home confinement program must continue but should be improved and become more selective about the kinds of inmates it takes.

State and county jails face severe crowding problems. It costs \$12.80 a day to keep an inmate on home confinement vs. \$67 a day to keep him in prison.

"We all believe this is a very worthwhile program," Kosco said. "We want it to continue in the state of New Jersey, but we want it to work as close to perfect as we can make it." Kosco said the program should be put "on hold" as Fauver had announced last month, but added, "We don't mean stopped." Kosco said the program should not be expanded but that as inmates come out of home detention, new inmates should enter. As of yesterday, 642 state inmates - all within six months of parole - had been released to home confinement with electronic monitoring. Some counties also use electronic bracelet programs.

Kosco and Sen. John Girgenti (D-Passaic) said the state should be more selective about the kinds of inmates it releases into the program. "I have problems when I read about people who were armed robbers who are now part of the program," Girgenti said. He said drug dealers and persons with ties to organized crime should also be ineligible for home detention. Girgenti and Kosco have introduced bills to restrict eligibility for home detention.

Fauver said he had canceled plans to expand the state's electronic anklet program in the next budget year. He added that he was "still confident" about the program but said it is better suited to county jail inmates than state prison inmates convicted of more serious crimes. Fauver said he was awaiting a consultant's report on the technical as pects of the home detention program and the procedures used in other states with similar programs.

#### No access to exchange via Cellnet

Lord Wodehouse <w0400@uk0x08.ggr.co.uk> 15 May 92 11:53:00 BST

Recently an old friend tried to call me at work, in response to a call from me. He discovered that his moble phone on the Cellnet network would not reach an 081-966-nnnn number, while he could do so from a standard BT phone. Being a comms specialist, he called Cellnet, after a discussion with me. The end result was that Cellnet had in fact left this exchange out of their routing tables. It is now in!

The reason behind this is that Cellnet (although partly owned by VBT) has to pay for any access to the BT phone network. To prevent calls being made to exchanges that do not exist and thus return a number unobtainable, but still raise a charge on Cellnet, but nothing that can be charged to the customer, Cellnet blocks such calls. When 966 came into being, no one added the route to make it available.

Lord John - The First Programming Peer on INTERNET!

## ✓ OTA has issued a report re "software property"

Jim Warren <jwarren@autodesk.com> Thu, 14 May 92 14:55:13 PDT

Hi, all. I just received this and tho't you'd be interested. --jim

>From autodesk!megalon!wsgr Thu May 14 08:31:36 1992To: megalon!jwarrenSubject: Software Patent Report

#### Jim -

Just in case you hadn't heard, Congress' Office of Technology Assessment has released a new report on the state of protection for computer software. According to an article in the Daily Journal, the report entitled "Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technology Change" has drawn praise for its sophisticated look at the unique problems in safeguarding technology rights.

The report is available through the U.S. Government Printing Office (\$11). - MarkB

#### Pentagon taps hackers to write viruses

John Mello <jmello@igc.org> Fri, 15 May 92 05:32:15 PDT

The following item is in the latest issue of Mother Jones. Cybervirus warfare anyone?

The Pentagon has a dream: An enemy soldier is attempting to pull up vital information on his computer screen. Suddenly, a peace sign flashes, along with the message, "You are STONED!" A virus has destroyed his files.

If you can make this dream a reality, Secretary of Defense Dick Cheney wants <it>you<>! His department's Innovative Research program is enlisting an unlikely group--computer hackers--to create strategic computer viruses that can attack enemy systems via radio signals. According to an official at the Army's Center for Signal Warfare, one hacker has already been awarded a \$500,000 contract for the program's production phase.

The exact nature of the work is classified, but the Signal Warfare official told <it>Mother Jones<> magazine that the virus project is based at Fort Monmouth, New Jersey, and described the work as "serious stuff.... Some believe these [viruses] exhibit lifelike tendencies, reproducing themselves like animals or plants."

Critics fear that the Pentagon's viruses pose a greater threat to computer networks at home than do any potential enemies overseas. Last year, for example, the "STONED!" virus and several others somehow found their way into nearly five thousand battlefield computers awaiting shipment to the Persian Gulf.

## Ke: Microsoft advocates killing of Jews (<u>RISKS-13.48</u>)

mathew <mathew@mantis.co.uk> Thu, 14 May 92 15:21:11 BST

I decided to see what other sinister secret messages were lurking in Windows 3.1's "WingDings" font.

If you type "IBM", you get a waving hand, a hand making an "OK" symbol, then a bomb. Obviously a reference to OS/2.

If you type "GOD", you get a hand pointing to heaven, a white flag, and a thumbs down symbol. Clearly Microsoft are a bunch of atheists.

If you type "MAC", you get a bomb, a V for victory sign, and a thumbs up. Plainly inspired by the recent legal bombshell in the look-and-feel lawsuit.

If you type "UN", you get a crucifix followed by a skull and crossbones. Obviously Microsoft knows something about the United Nations that we don't.

Another potentially interesting bit of information: In the beta-test versions of Windows 3.1, three "dingbats" fonts were supplied -- Lucida arrows, Lucida stars and Lucida icons. WingDings seems to have been formed by condensing the three into one single font. It's interesting to note that whereas Lucida icons had both black and white coloured hand symbols, WingDings has only the white-skinned variety.

mathew [Clever disclaimer omitted, as usual]

### \* Two privacy newsgroups [Don't confuse them.]

"Peter G. Neumann" <neumann@csl.sri.com> Sat, 16 May 92 14:33:46 PDT

Following are items relating to two different newsgroups on PRIVACY.

Dennis Rears' DIGEST is purposefully on the permissive side, less stringently moderated than RISKS; it is ideal for people who want relatively open newsgroups. Lauren Weinstein's FORUM will be on the selective side, substantially more closely moderated than RISKS; it is suitable for people who have little time, but have a vital interest in privacy. Both gentlemen are serious in their efforts. I think there are many reasons for both groups to coexist. Perhaps one or the other will satisfy those people interested in privacy issues who complain to RISKS that they want LESS MODERATION or MORE MODERATION, respectively.

I hope that general discussions on privacy issues will continue to appear in RISKS, because those issues represent serious risks. Perhaps both moderators will submit summaries of key discussions to RISKS for our wider audience.

#### Announcing the PRIVACY Forum digest!

<privacy@cv.vortex.com> Wed, 13 May 92 00:08:14 PDT

Announcing the global Internet PRIVACY Forum!

The PRIVACY Forum is a moderated digest for the discussion and analysis of issues relating to the general topic of privacy (both personal and collective)

in the "information age" of the 1990's and beyond. Topics include a wide range of telecommunications, information/database collection and sharing, and related issues, as pertains to the privacy concerns of individuals, groups, businesses, government, and society at large. The manners in which both the legitimate and the controversial concerns of business and government interact with privacy considerations are also topics for the digest.

Except when unusual events warrant exceptions, digest publication will be limited to no more than one or two reasonably-sized digests per week. Given the size of the Internet, this may often necessitate that only a small percentage of overall submissions may ultimately be presented in the digest. Submission volume also makes it impossible for unpublished submissions to be routinely acknowledged. Other mailing lists, with less stringent submission policies, may be more appropriate for readers who prefer a higher volume of messages regarding these issues.

The goal of PRIVACY Forum is to present a high quality electronic publication which can act as a significant resource to both individuals and organizations who are interested in these issues. The digest is best viewed as similar in focus to a journal or specialized technical publication. The moderator will choose submissions for inclusion based on their relevance and content.

The PRIVACY Forum is moderated by Lauren Weinstein of Vortex Technology. He has been active regarding a wide range of issues involving technology and society in the ARPANET/Internet community since the early 1970's. The Forum also has an "advisory committee" consisting of three individuals who have offered to act as a "sounding board" to help with any questions of policy which might arise in the course of the Forum's operations. These persons are Peter Neumann of SRI International (the moderator of the excellent and renowned Internet RISKS Forum digest), Marc Rotenburg of Computer Professionals for Social Responsibility (a most clear and articulate spokesman for sanity in technology), and Willis Ware of RAND (one of the U.S.A.'s most distinguished champions of privacy issues).

Feel free to distribute this announcement message to any interested individuals or groups, but please keep this entire message intact when doing so. Thanks!

How to subscribe to PRIVACY Forum

Individual subscriptions for the PRIVACY Forum are controlled through an automated list server ("listserv") system.

To subscribe, send a message to:

privacy-request@cv.vortex.com

or:

listserv@cv.vortex.com

with a line in the BODY of the message of the form:

subscribe privacy

### ✓ Computer Privacy Digest/comp.society.privacy

"Dennis G. Rears " <drears@pica.army.mil> Wed, 13 May 92 13:59:53 EDT

I am the moderator of the Computer Privacy Digest. The computer Privacy Digest is an Internet mailing list that is dedicated to the discussion of how technology impacts privacy. This list is gatewayed into the moderated USENET newsgroup comp.society.privacy. In lot of ways it is a subsection on the risks digest but it concentrates on the risks of technology on privacy. The charter is:

comp.society.privacy Effects of technology on privacy (Moderated)

This newsgroup is to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. This newsgroup will be gatewayed to an internet mailing list.

Submissions go to: comp-privacy@pica.army.mil and administrative requests go to comp-privacy-request@pica.army.mil.

dennis

Dennis G. Rears MILNET: drears@pica.army.mil UUCP: ...!uunet!cor5.pica.army.mil!drears INTERNET: drears@pilot.njin.net USPS: Box 210, Wharton, NJ 07885 Phone(home): 201.927.8757 Phone(work): 201.724.2683/(DSN) 880.2683 USPS: SMCAR-FSS-E, Bldg 94, Picatinny Ars, NJ 07806

### MDC, the C-17 and the F-15E

<John\_Karabaic@NeXT.COM> Fri, 15 May 92 10:57:17 EDT

>END OF STORY. Mark Seecof asks: has anyone seen the report itself? >I'd like to know in what way it was a mistake to give McDonnell-Douglas >control over software development for a plane it was building?

---flame on

Well, since I was the Software Manager on the F-15E I can give you lots of reasons from personal experience about why any Government agency should think long and hard before giving McDonnell Douglas control over any software project:

1. Their insistence that flight-control software is not flight-safety critical, since there was a hydraulic backup in the F-15E aircraft.

2. Refusal to perform software Formal Qualification Tests prior to first flight, stating that the FQT is required only on production aircraft, and F-15E-1 was not a production aircraft. FQT should be an iterative testing process, but according to MCAIR, it was an acceptance test.

3. Refusal to define software stored in ROM as software, defining it instead as "firmware", and thus not subject to formal review and testing.

These are just a few off the top of my head, five years after the fact. Don't get me wrong; I think MCAIR did a fantastic job on the F-15E. It's one great weapon system. But McDonnell Douglas's biggest problem on the F-15 project was, even though they could build excellent aircraft and systems, they wouldn't tell us government types (including this pitiful second lieutenant) anything unless we pried it out of them with a crowbar. And sometimes not even then, parroting the tired line, "Out of scope [of the contract]!" This makes it extremely difficult to get enough information to enable "organic support" (support by US Government personnel) or second-sourcing of software after the systems are delivered. Since the Advanced Tactical Fighter Program Office was right across the hall at that time, every time I had a problem, I would go tell the people writing the contracts for that program how responsive my contractor was being. (In Air Force talk: "Check six!")

#### --flame off

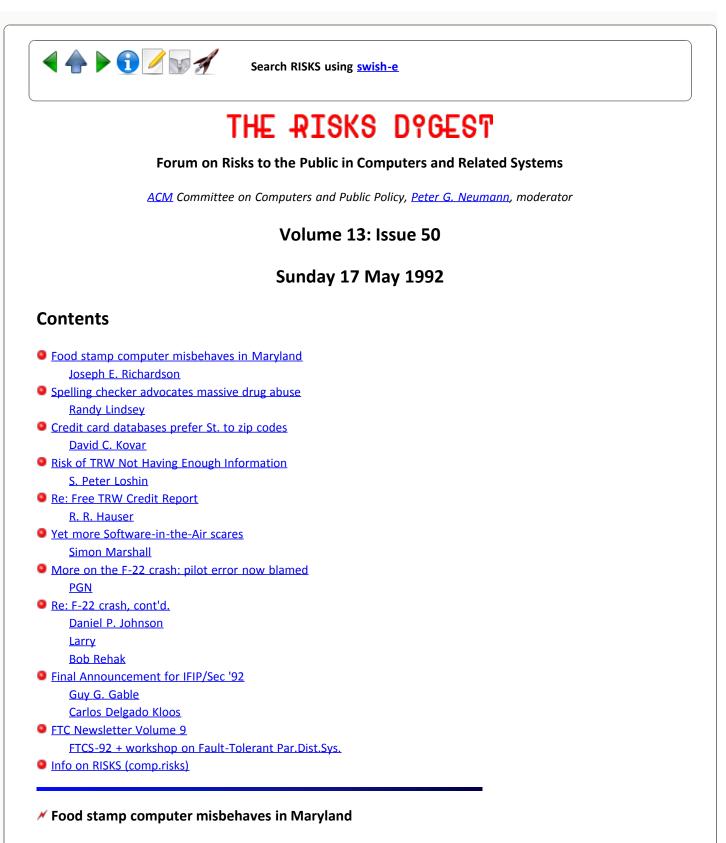
But there may be another, more simple reason for the GAO's finding: I believe that the US Government, not the prime contractor (MDC, in this case) has "total system performance responsibility" for the C-17. That is, a program office residing at Wright-Patterson AFB has the responsibility for integrating and testing every aspect of the aircraft, not the contractor who is building it. Since software is the glue that holds a modern military aircraft together, this may be why the GAO is faulting the C-17 SPO for not "controlling" the software.

John S. Karabaic, Systems Engineer, jkarab@NeXT.com, 513 792 5904 NeXT Computer, Inc.; 4434 Carver Woods Dr.; Cincinnati, OH 45242 cellular: 513 532 0224; fax: 513 792 5913; territory: OH, IN & KY



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Joseph E. Richardson <joseph@bse.com> Wed, 13 May 92 09:43:21 EDT

Food Stamp Computer Clogs in Md. -- Overloaded System Causes Long Lines By Retha Hill - Washington Post Staff Writer [Washington Post, 13 May 1992]

Maryland food stamp clients using a new electronic benefit system were unable

to buy groceries [on 6 May 1992 <JR>] after the state-of-the-art computer system failed, causing long lines at hundreds of stores in the state.

The system, which the U.S. Department of Agriculture has said it plans to use as a model for the rest of the coutry, became overloaded for the second time in a month and shut down for about two hours as hundred, and possibly thousands, of recipients tried to use their plastic benefit cards to make purchases. Typically, the first few days of the month are heavy shopping days because that is when clients receive benefits.

The system "reached a point where it clogged," said Helen Szablya, a spokeswoman for the Maryland Department of Human Resources. She said that she did not know if other benefits that are encoded on the plastic cards, such as welfare payments and child support, were affected.

About 31,000 Maryland residents in Montgomery, Prince Georges and Cecil counties and Baltimore now have the cards. Clients in Baltimore, Howard and Anne Arundel counties are to get the cards by mid-summer, and eventually 200,000 recipients will use them.

Szablya said the electronic benefit transfer system is better than the old method [Electronic systems are always "better", aren't they? :-) JR] of issuing coupons to clients and said that problems are going to happen because it is the first of its kind in the country. The system last stopped working April 11 for about two hours. "It's going to have a few blips. We are happy with the fact that we haven't had more," she said.

Shoppers and grocery store officials complained of long lines and carts loaded with groceries abandoned as checkout stations. Food stamp clients were given \$50 vouchers to make purchses, but cashiers had to call a toll-free number to verify each transaction.

"We just think it's unfortunate that this happens and that it inconveniences our customers," said Mitchell D. Herman, senior vice president for corporate affairs for Shoppers Food Warehouse. [How true, how true. -- JR]

Joseph E. Richardson, Berard Software Eng., Inc., 101 Lake Forest Blvd, Ste 360, Gaithersburg, MD 20877-2611 (301) 417-9884 joseph@bse.com

### Spelling checker advocates massive drug abuse

Randy Lindsey <lindsey@tincup.enet.dec.com> Tue, 12 May 92 12:57:56 PDT

It is not uncommon in large companies to require an annual "payout", in which each employee picks up their paycheck in person, displaying ID. I think this is to guard against payroll padding.

At the facility where I'm doing a project, all 1,500 employees received a memo ordering them to report to the cafeteria for their annual "peyote". Peyote appeared several times in the memo, and even in the title line! Eventually one of my colleagues ran "payout" through the spelling checker, and sure enough it suggested "peyote" as the alternative.

Perhaps the spelling checker writers are junior staff with closer ties to their college counter-cultural days than to corporate terminology... Randy Lindsey

#### ✓ Credit card databases prefer St. to zip codes

"David C. Kovar" <kovar@eclectic.com> Wed, 13 May 1992 09:38:32 -0400

About two years ago, I started getting some credit card statements a few days late. All of them had an incorrect zip code and the post office had corrected them by hand and resent them. I called up the offending credit card companies and tried to correct the problem. Two of them corrected it, one of them couldn't/wouldn't. I eventually cancelled the card belonging to the bank that couldn't get the address right.

Well, for various reasons, I've taken my time in paying off the account, so I still get statements from them, still with the wrong zip code. Apparently the Post Office is cracking down on bad zip codes because both AT&T and this particular bank called me up this week to verify my address.

About three months ago I finally figured out what I thought was the problem. I live on Broadway, and my zip code is 02174. People frequently want to know if it is Broadway Rd, Broadway St, Broadway Ln? It's just Broadway. All of the offending statements had my address as Broadway St, and my zipcode as 02111. Someone's database, somewhere, mapped Broadway St. to a 02111 zip code and, if the zip code was corrected but the street address wasn't, it would modify the zip code again to what it believed was correct.

So, I explained all this to the person from the bank, had her change the street address and the zip code, and we'll see if it works.

If anyone has any more information on this problem, I'd be interested in hearing about it. I don't have enough time at the moment to track down which database these guys are using. If anyone is curious, the bank is Chase Manhattan.

-David Kovar

[We have had a spate of similar tales of woe in the past. In this case, please send responses to David. If anything exciting comes up, I am sure he will share it with us. PGN]

### Kisk of TRW Not Having Enough Information

"S. Peter Loshin" <pql1191@mvs.draper.com> Tue, 12 May 1992 16:20:00 EDT

This might be of some interest, as I recently was denied credit (temporarily) due to inability of the credit grantor to verify my address. I cleared that up

by sending copies of utility statements to the credit grantor, but out of curiosity I took advantage of the free copy of the TRW credit report that caused the denial.

Maybe I'm just different - I use my middle name and don't use my given first name, and I use a PO box for as much correspondence as possible - but the report was VERY sparse. My address was three years out of date and they had no info on my employer or on any of the credit cards that I customarily use. There were NO negative reports from any of the institutions listed, and only one neutral report.

Overall, I was fairly pleased with the lack of complete information on me unless it was all a ruse to lull me into a false sense of security about my privacy.

Peter Loshin | peter@draper.com | 555 Technology Sq Cambridge MA 02146

### Re: Free TRW Credit Report (<u>RISKS-13.46</u> and 47)

R. R. Hauser <rrh@gabriel.b11.ingr.com> Fri, 8 May 1992 13:03:45 -0500

Three credit reporting agencies exist (to my knowledge): TRW, Transunion (Merchants), and Holloway Credit Bureau.

Since I happen to have my credit report in hand (Holloway) which lists address/phone for Transunion and TRW, I called TRW long-distance and spoke with a representative about the free credit report. She gave me this number 1-800-392-1122.

The risk seems low IF you do the following rather than trusting some bulletin board posted P.O. Box address.

Go to a local credit bureau and get your report (~\$10) or borrow someone's to get valid address/phone for TRW. Call and inquire.

Since this may cost a bit you could call the 1-800 number I got from TRW and wait until a representative comes on. The risk in trusting this posted phone number can be reduced by waiting until a person comes on rather than trusting a computerized voice.

When questioned, the TRW representative (how knowledgeable?) implied that \_establishing\_ any kind of credit had nothing to do with this service. Also, a bill is not necessary ... just anything with the name-address linkage. Hmmm...

Seems that the risk of someone easily obtaining your credit report from TRW may be higher now.

R. R. Hauser DOMAIN: hauserr@infonode.ingr.com

# Yet more Software-in-the-Air scares

Simon Marshall <S.Marshall@sequent.cc.hull.ac.uk> Sun, 17 May 1992 16:06:12 +0000

Here are yet more stories concerning flight control software going wrong in commercial passenger aircraft. It is taken from the front page of the UK ``Sunday Telegraph'' May 17, 1992, a so-called ``quality newspaper''. The article is quoted in its entirety.

Air scares over computers", Robert Matthew and Christopher Elliott.

A spate of software errors forcing planes into sudden changes of speed and direction has rekindled concern about the use of computers by the aircraft industry. An internal British Airways document discloses 10 serious incidents involving computer errors in January, including:

- January 13, when the flight-management system on a Boeing 747-400 from Washington to Heathrow suddenly ordered a speed reduction of 50 knots.
- January 26, when a Boeing 747-200 flying to Gatwick from Barbados experienced a sudden increase in thrust due to a software error.
- January 27, when a Boeing 747-200 from Manchester to Islamabad suddenly pitched upwards. The crew had to turn off the auto-pilot to bring the aircraft back into normal flight.

Other computer errors have led to navigational deviations and to the auto-pilot wandering from the correct route.

British Airways said action had been taken to rectify the problems, which did ``not present any threat to the safety of the aircraft". A spokesman added that the software had Civil Aviation Authority approval and had been tested by BA for more than 100 hours before entering service.

But leading computer experts are worried that there is no adequate way of testing the enormously complex software routinely used by the aircraft industry.

The British Computer Society will call this week for international standards on the design of safety-critical software, and for special qualifications from [sic] those working the field.

Professor John Cullyer, of Warwick University, chairman of the society's Safety Critical Systems Task Force, said: ``We haven't for enough highly educated and trained checkers. We actually know what we ought to be doing but we just don't have enough men and women sufficiently qualified.''

Professor Bev Littlewood, of City University, London, has told the American Association for Computing Machinery that the aircraft industry could not substantiate claims for computer reliability."

There are couple of things that made me post this article. Firstly, the number

of incidents - 10 in a single month with BA. This implies that software is not working in normal, routine, flying conditions, where you might expect the behaviour of such systems to be correct. There are no suggestions in the article that "the pilot flew to low", "the pilot applied full thrust too late", and so on, but that the systems themselves failed to perform correctly in normal conditions.

The second is that at least some of the "software errors" were within auto-pilot control systems (it may be all, the article is not clear - maybe BA does not fly any fly-by-wire aircraft anyway, I don't know). These systems are, as I understand it, typically not used for takeoff or landing, but to fly from A to B once airborne. Given the number of years these systems have been around, it worries me to think that these relatively simple systems fail at this frequency, while fly-by-wire, with its increased complexity and the increased reliance upon those systems for the safety of the aircraft, is now being applied to commercial aircraft.

The third is that the software had "CAA approval", as if this is meant to make us feel any better, and that it had been tested by BA themselves (not the CAA), for "100 hours before entering service". This does not seem particularly rigorous to me!

The fourth came with the old call for qualifications for those working in safety-critical software design; lack of suitably trained people. Maybe the CAA and aircraft manufacturers should be training their software personnel?

Simon Marshall, Dept. of Computer Science, University of Hull, Hull HU6 7RX, UK Email: S.Marshall@Hull.ac.uk Phone: +44 482 465181

#### More on the F-22 crash: pilot error now blamed (<u>RISKS-13.46</u>)

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 14 May 92 12:10:56 PDT

Those of you who read <u>RISKS-13.46</u> noted that computer software seemed to be implicated in the crash of the only flying F-22 prototype. A later report now suggests pilot error. As usual, the real causes are probably some combination of a poorly designed human interface, software design and implementation problems, hardware-software system response delays, and pilot problems (training, complexity, etc.).

An AP report somewhen during 11-13 May (while I was in D.C.) had these statements (starkly excerpted):

A new Air Force videotape of the crash, shot from the plane's side, shows the radar-eluding aircraft with its landing gear down as it nears the runway at the California base. The landing gear is then drawn back up about the same time the afterburners go on. The plane then bucks wildly before hitting the pavement, sliding several thousand feet and burning. [...]

Congressional sources, who requested anonymity, said the Air Force now suspects that pilot error caused the crash. A final report is not expected for several weeks after the Air Force completes its investigation.

Air Force Chief of Staff Merrill McPeak [quoted in <u>RISKS-13.46</u> as hoping that it was software, because that would be "relatively straightforward" to fix] testified before Congress he suspected the crash was the result of a mechanical malfunction in the plane's computer system. "I am utterly convinced personally that this is a very meritorious design," said McPeak [...]. The Air Force chief of staff said he saw no need to change the program, which calls for 650 of the fighter planes to become operational in 2002.

#### Ke: F-22 crash (Watson, <u>RISKS-13.47</u>)

<drdan@src.honeywell.com> Mon, 11 May 92 09:08:43 CDT

I haven't entered this discussion because there are a lot of people with more solid credentials, but there are some elementary points to be made. If I get my ears pinned back, so it goes.

When something goes seriously wrong in a control system, a common result is that the system goes unstable. The wild motions of the tail are due to positive feedback between the control system, the pilot, and the aircraft responses. As to what caused the instability, it can be almost anything, software error, design error, hardware failure.

A likely explanation would be that the aircraft had some unexpected aerodynamic characteristics in the low altitude, high weight regime that it was flying (to be expected in a prototype aircraft, that's how test pilots earn their pay). The result was a "PIO" (Pilot-Induced Oscillation).

One can view this as a software error since the fix is to change the software to allow for the unexpected dynamics, or as a pilot error since he was part of the positive feedback loop, but it is better to classify it as a design problem since one of the goals of the design is to avoid creating a situtation in which a PIO is possible.

Daniel P. Johnson, Honeywell Systems and Research Center, MN65-2500, 3660 Technology Drive, Minneapolis, MN 55418 drdan@src.honeywell.com 612-782-7427

### Ke: F-22 crash, cont'd. (Watson, <u>RISKS-13.47</u>)

<larry@psl4381.NMSU.Edu> Wed, 13 May 92 13:23:50 MDT

I recorded the same footage and played it several times in slow motion to observe the porpoising motion of the ship. A flash from the cockpit (assumed to be the ejection system) could be seen at the end, just before the ship kissed the runway.

I believe you'll find that large, rapid movements of control surfaces are a common feature of modern fly-by-wire control systems for fighters. It is necessary because of the complex flying modes involved, particularly on

take-off and landings, which limit control surface effectiveness. Special [non-linear] servo modes are involved.

Such problems are likely to be exacerbated on the YF-22 which is probably an unstable design to begin with (to achieve maximum maneuverability) stabilized by the computerized control system.

> Odd that the software should be seen as a possible cause of the crash, ...

You can almost bet that the pilot was NOT the problem. The handful of people who can qualify as test pilots are not the sort to make the mistake of extreme pilot input. Many have been known to cooly report problems and symptoms in the last few seconds of their lives.

As for software, someone observed that if buildings were constructed like programs, the first woodpecker to come along would destroy civilization! (Still, I would expect this particular control program to be a state of the art example of good software..)

> I though most aircraft could dump/vent excess fuel, you don't have to be at low> altitude to do this, do you?

That's another problem. Suppose we suddenly reduce the flight weight of a fighter by a significant percentage? It seems reasonable that the ship might need to be retrimmed quite a bit after a major fuel dump, so it is probably not prudent to do it at low altitudes.

Larry

### Ke: F-22 an speaking out of turn (Watson, <u>RISKS-13.47</u>)

Bob Rehak Ext. 3-9437 <A20RFR1@niu.bitnet> Mon, 11 May 92 10:15 CDT

All well designed aircraft have a fuel jettison system for dumping fuel. Most fuel is dumped at higher altitudes so that it evaporates before it hits the ground; however, if your aircraft is in distress and is at a low altitude and you are someplace isolated like the F-22 was, who cares if you jettison the fuel.

The claim that the F-22 was doing these low altitude high speed passes to reduce its fuel load so it could land with a greater saftey margin sounds bogus to me. If the aircraft was in distress these aren't the kind of maneuvers a prudent pilot would be doing.

Also, what about the risks of speaking out of turn. I feel Gen. McPeak's statements are a bit premature and could bias the accident investigators. I don't how many times I have gone done the wrong path in tracking down a software problem because I was biased by the information given to me by a software developer (who's judgement, expertise, ect. I trusted). Moral of the story, start at the beginning and follow your judgement not theirs. If the investigators were to think: Hey, let's look at the s/w and computers because that's where the Gen. says the problem is... well you know what happens next.

Bob Rehak, DBA At Large, A20RFR1@MVS.CSO.NIU.EDU

## Final Announcement for IFIP/Sec '92

"Dr. Guy G. Gable, IFIP/Sec '92 Program Chair" <ISCGUYGG@nusvm.bitnet> Sat, 16 May 92 07:24:36 SST

> THE IFIP/SEC'92 8th INTERNATIONAL INFORMATION SECURITY CONFERENCE

> > May 27-29, 1992 Raffles City Convention Centre Singapore

[FULL TEXT IS FTPable from CRVAX, cd RISKS: , file IFIP.1992 , or get it from Guy Gable. PGN]

## // IFIP'92 registration form

Carlos Delgado Kloos <cdk@dit.upm.es> Thu, 7 May 92 19:47:27 +0200

[FULL TEXT IS FTPable from CRVAX, cd RISKS: , file IFIP.1992 , or get it from Carlos Delgado Kloos. The DEADLINE FOR EARLY REGISTRATION DISCOUNT is 25 May. NEXT MONDAY!!! PGN]

# FTC Newsletter Volume 9

FTCS NEWS <ftcsnews@snowy.crhc.uiuc.edu> Thu, 23 Apr 92 11:34:32 CDT

ELECTRONIC NEWSLETTER ON FAULT-TOLERANT COMPUTING

VOLUME 9, APRIL 1992

EDITOR: Prith Banerjee, University of Illinois

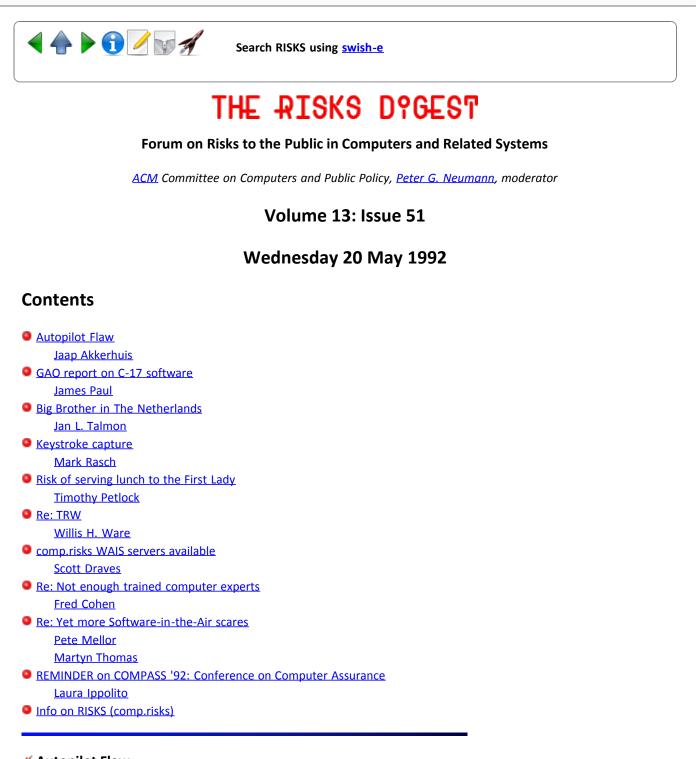
CONTENTS: (Each item can be searched by keyword ITEM and separated by a line of =======)

- 1. GENERAL INFORMATION AND REGISTRATION FOR FTCS-92,
- 7-10 JULY 1992, The Lafayette Hotel, Boston, Massachusetts USA
- 2. ADVANCE PROGRAM FOR FTCS-92
- 3. WORKSHOP ON FAULT TOLERANT PARALLEL DIST. SYS. Campus Center Hotel, Amherst, Massachusetts USA, July 6-7, 1992

4. CALL FOR PAPERS (HICSS-26) DEADLINE EXTENSION

5. COURSE ANNOUNCEMENT (FAULT-TOLERANT DISTRIBUTED COMP.)





## 🗡 Autopilot Flaw

Jaap Akkerhuis <jaap@research.att.com> Mon, 18 May 92 12:31:33 D

Older Boeing 747 Airplanes Suspected of Diving Due to Design Flaw

SEATTLE (AP) - The Boeing Co. should redesign the autopilot system on hundreds of 747 jumbo jets because of a flaw that could send the planes into a dive, the National Transportation Safety Board said.

The board has asked the Federal Aviation Administration to order the

redesign, NSTB chairwoman Susan Coughlin said Thursday.

The board investigated an incident in December in which a 747-100 cargo jet rolled to the right and dove 10,000 feet from an altitude of 31,000 feet while on a flight from Anchorage to New York.

Stray signals told the autopilot to put the plane into a roll, according to Coughlin, who cited tests by Canadian authorities on the Evergreen International Airlines aircraft. It is unknown what caused the signals, she said.

The plane landed safely.

The FAA will decide within 90 days whether to order the redesign, spokesman Dave Duff said.

"We believe the autopilot system is safe," Boeing spokesman Chris Villiers said.

The NTSB request includes the systems on 724 airplanes delivered between 1969 and the late 1980s. A different autopilot system is used now.

#### ✓ GAO report on C-17 software

James Paul <jpaul@nsf.gov> Mon, 18 May 92 11:58:45 EDT

Those interested in the C-17 software report from GAO can get a free copy by calling (202) 275-6241 and asking for report IMTEC-92-48, dated May 7, 1992. The title is "Embedded Computer Systems: Significant Software Problems on C-17 Must be Addressed." Alternatively, call your Congressman's or Senator's district office and ask them to get it for you from GAO.

P.S. [for PGN, but relevant here in case you try to send mail to James!] [For reasons DELETED, ] messages going to PAUL@NOVA.HOUSE.GOV have been wafting off into the electronic ether somewhere. We are supposed to be back on-line again sometime soon, but until then I've been downloading RISKS from the archives to try and keep up. You'll love the C-17 report -- GAO says "The C-17 is a good example of how \_not\_ to approach software development when procuring a major weapons system." It has most of the usual problems -- underestimated risks, failure of the customer to exert control, poor documentation. Great reading material for classes in software development.

-- James Paul (House Science Committee)

#### Main Big Brother in The Netherlands

"Jan L. Talmon" <MFMISTAL@rulimburg.nl> Tue, 19 May 92 09:18 MET

In today's [19th of May] issue of the "Volkskrant", a quality Dutch newpaper there appeared an article which says that the Departments of Justice and Traffic are studying the possibility to introduce smart cards to detect, among other things, violations of the traffic laws such as speeding (quite common on the Dutch highways), crossing red lights, frauds with number plates etc. The other things that could be controlled is whether the car owner has paid his insurance fee (obligatory in The Netherlands), his road tax, and whether the car has had it's yearly technical check (APK).

The system under study consists of a smart car to be attached to the car, detectors in or near the roads and a central computer system.

The article says: "A major drawback is the possible feeling that `Big Brother is watching you'. By installing a privacy code, data on law violations will only be transferred to the relevant organizations. Another problem is the value of information obtained by electronic means and stored in magnetic form in court. Currently, it is up to the judges to value the information provided by computer systems."

The article ends with: "The organizational consequences, however, are still completely unclear. Of course, attention should be paid to the protection of the system against tampering."

Risks.... obvious!!!

Jan Talmon, Dept. of Medical Informatics, University of Limburg, MaastrichtThe NetherlandsEMAIL: Talmon@MI.Rulimburg.nl[Translated by JT]

#### 🗡 Keystroke capture

<Rasch@DOCKMASTER.NCSC.MIL> Wed, 20 May 92 16:03 EDT

There has been a lot of talk on the net, (and off the net) about whether or not it is legal or proper for a system administrator to capture keystrokes of intruders/trespassers who are using their system to break into the systems of others. We all remember Cliff Stoll's exploits in "The Cookoo's Egg" where he traced the German Hackers through LBL by keystroke capture, and then notified downstream users that they were being attacked.

Several people (and organizations) have taken the position that keystroke capture both violates privacy rights and constitutes illegal electronic surveillance. I believe that, with respect to \*intruders\* both these arguments are specious.

Fourth Amendment

The principal protection against \*governmental\* intrusions into privacy rights is the Fourth Amendment to the constitution which provides that:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

It is important to note that this only applies to searches performed by the government. Burdeau v. McDowell, 256 U.S. 465, 475 (1921) even if the

government is not acting in a law enforcement capacity New Jersey v. T.L.O., 469 U.S. 325, 336 (1985). Thus, to the extent a sysop is not a "government agent" the Fourth Amendment is not implicated.

Also, in order for there to be a Fourth Amendment violation, the individual must have exhibited an actual subjective expectation of privacy (Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring)) and society must be prepared to recognize that expectation as objectively reasonable. An intruder should have neither a subjective expectation of privacy, nor should society recognize any expectation of privacy as "reasonable." Thus, if you break into my system, I should be able not only to kick you off, but also to monitor what you do on my system.

Finally, the general sanction for violation of the Fourth Amendment is suppression of the illegally seized evidence and its fruits. Weeks v. U.S., 232 U.S. 383, 398 (1914) (federal search); Mapp v. Ohio, 367 U.S. 643, 655 (1961) (state search). Thus, a private keystroke capture of an intruder would not violate the Fourth Amendment.

#### **Electronic Surveillance**

In 1986 Congress amended the Electronic Communications Privacy Act to prohibit the unlawful interception of electronic communications, including e-mail and the like. In general, the law, contained in Title 18 of the United States Code, Section 2511, prohibits the interception of wire, oral or electronic communications. HOWEVER, there are several provisions which would permit keystroke monitoring in certain circumstances.

#### First, 18 U.S.C. 2511(2)(a)(i) notes that:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service [bbs operator] . . . to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is necessarily incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

While this statute is not a model of clarity, and fails to define key terms like what is a \*provider\* of electronic communication service (the network administrator? the sysop?) it appears to permit electronic interception and keystroke capture it this is necessary to protect the rights and property of the provider of the service. If the intruder is breaking in to the computer of \*another\* (not the provider) and the provider can easily terminate this unauthorized use, then it could be argued that the keystroke capture is not necessary to protect \*his\* property. However, the statute uses the term "necessarily incident to . ." not "necessary to" and, in light of the strong possibility of downstream liability to the provider for somehow permitting the intruder to use his system to break into another's, a strong argument can be made that keystroke monitoring of intruders is reasonable, prudent, and necessarily incident to the protection of rights and property.

In addition, 18 U.S.C. 2510(13) defines a "user" of electronic communications as:

any person or entity who -

- (A) uses an electronic communication service; and
- (B) is duly authorized by the provider of such service to engage in such use.

Since an intruder is not authorized to use the service, he is not a "user" entitled to protection under the statute. Finally, while warning banners are helpful to demonstrate a lack of authorization to use a particular system, they are not required to demonstrate a lack of authorization any more than "No trespassing" signs are necessary to demonstrate a lack of authorization for an individual to, for example, break into your house. (a simplistic analogy admittedly)

This is, of course, only part of the story. Many states have privacy statutes, and their own definitions of illegal electronic interception, and this does not address potential civil liability to users for excessive keystroke capture. However, I believe that if keystroke monitoring is accomplished in a reasonable and prudent fashion, it would not run afoul of either the constitutional or statutory provisions. Let the trespasser beware!!!

Mark Rasch, Esq., Arent Fox Kintner Plotkin & Kahn [Std. Disclaimer]

### Kisk of serving lunch to the First Lady

Timothy Petlock <timdude@cs.wisc.edu> Mon, 18 May 1992 17:25:32 GMT

Yes, that's right. Serving lunch to Barbara Bush can cause all sorts of problems from the past to be dug up. My roommate and I found out firsthand on Saturday afternoon. He called me 20 minutes after I dropped him off at work, saying "It seems I'm in jail. Can you come downtown and bail me out? Bring \$220."

The cause? It seems they did a background check on all the hotel employees that would be involved in the function that day. He had bounced one too many checks at a grocery store in the northern Wisconsin town where he lived -- a year and a half ago. The checks were all paid before he moved down here and he had no idea that any charges had been filed.

### Re: TRW (Culnan, <u>RISKS-13.48</u>, Loshin, <u>RISKS-13.50</u>)

"Willis H. Ware" <willis%iris@rand.org> Mon, 18 May 92 11:05:38 PDT

Mary Culnan reported the lengthy list of items that TRW asks for in order to receive the free credit report. Peter Loshin reported that he found

his credit report satisfyingly "sparse". TRW is reported to be in the information-sales business which would imply large and quite complete records. How does one reconcile all of that?

The Fair Credit Reporting Act requires that a copy of the "credit report" be given to anyone upon request [or for fee] or upon denial of credit. At the time the FCRA was passed [roughly 1970], things were simple in the credit-reporting and information business. They are not today.

One must wonder what the definition of "credit report" would be in today's world. I'm sure that the TRWs of the world would argue that it would be just that part of a data-subject's record that is pertinent to a credit decision. It is unlikely that any data-subject gets the full content of the record by requesting a credit report, although it is tempting to believe to the contrary.

I know of no law compelling the credit reporting industry to go beyond furnishing the most simplistic from of an individual's record; namely, that part of the record pertinent to credit matters. One does not know what the status of the individual's total record might be. We're not seeing them, but it's obvious that they're available for sale. Might they be subject to subpoena without knowledge of the data-subject? One wonders what corporate or industry policy is on that count.

Of course not everything need be included in a single record. A company could maintain separate databases -- although perhaps less efficiently -- for credit reporting vs. general information sales. Of course, modern software can easily subset a record for printing, but it really doesn't matter from the viewpoint of the data-subject who is not seeing everything. Willis Ware, Santa Monica, CA

#### comp.risks WAIS servers available

Scott Draves <spot@FORTRAN.FOX.CS.CMU.EDU> Sun, 17 May 92 22:33:54 EDT

The RISKS digest is available via WAIS. there are two servers, one run by TMC and one by me. TMC's is better, but is available only during restricted hours.

WAIS is a distributed full-text search system based on the Z39.50 protocol. There are on the order of 200 public servers scattered around the world which provide a straightforward way to search through mailing list and newsgroup archives, network directories and catalogs, poetry, weather, back issues of the Communications of the ACM, and a variety of other stuff.

For more information, ftp to think.com then "cd wais". or see the comp.infosystems.wais newsgroup.

Below are the "source" files for the two servers:

(:source :version 3 :ip-address "128.2.206.11"
:ip-name "gourd.srv.cs.cmu.edu"
:tcp-port 6000
:database-name "comp.risks"
:cost 0.00
:cost-unit :free
:maintainer "spot@cs.cmu.edu"
:description "Server created with WAIS release 8 b4.1 on
May 9 21:58:25 1992 by spot@gourd.srv.cs.cmu.edu
The files of type mail\_digest used in the index were:
/gourd/usr0/spot/wais-db/comp.risks

This server contains issues 1.00 to (at least) 13.47 of the comp.risks newsgroup/mailing list:

FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

This server runs 24 hours everyday (cf risks-digest.src).

```
)
```

(:source :version 3 :ip-address "131.239.2.110" :ip-name "cmns-sun.think.com" :tcp-port 210 :database-name "RISK" :cost 0.00 :cost-unit :free :maintainer "bug-public@think.com" :description "Connection Machine WAIS server. Operated between 9AM and 9PM EST.

Risk Digest collection from the arpa-net list, but this is so far an unofficial archive server. It contains all issues, but is not updated automatically yet.

)

### Mot enough trained computer experts (Marshall, <u>RISKS-13.50</u>)

fc <FBCohen@DOCKMASTER.NCSC.MIL> Mon, 18 May 92 07:16 EDT

How true - but the root cause of the current software crisis (which is widely unknown to the user community) is that it's bad for business to talk about the down side. Let me give a few examples:

I was writing a monthly column for a rag in the Unix world, and it was cancelled because (according to the publisher) the advertisers threatened to pull their ads if the security problems with Unix were published in the rag. This despite the fact that I included code to fix every problem I described in the same article as I described the problem.

I was writing a monthly column for another rag in the Netware world, and the Novelle lawyers told the publication they would sue if my articles were not stopped! It seems they were upset that I was pointing out how netware could be abused and how to avoid the problems inherent in the implementation. Ther goes another forum for the public.

Over the last several years, I have applied for positions in over 100 universities, and the universal response is that protection is not of interest to the university community. This dispite the recent report from the US National Research Council that calls for increased university research in the field.

You cannot find a single US university (and only a few outside the US) with more than 2 computer security experts on the same faculty. You also cannot find a university in the US where more than one person was hired with the prior knowledge that they have computer security interest (again I am talking about faculty positions). With the educators woefully ignorant, we can only expect the students to be equally ignorant.

I have dealt with literally hundreds of companies over the last 10 years in the area of computer security consulting, and the universal feeling seems to be that you only invoke security after a disaster forces you to, and then you back away from it as soon as possible afterwards. It's like insurance, except that the board won't force you to get it, and the stockholders are never told that it's imprudent not to have it.

The media constantly hits the idea that any security system can be broken and that the human end of things saves the day. This makes the technological end of protection a negative in most people's minds. The social implication is that regular people rarely see any benefits with protection systems. How come we never hear on the risks forum about any successes where the computer security system saves people? It happens every day you know. How about a few nuclear reactor stories where human error was detected and corrected by a computer and saved us from a meltdown? How about some airplane stories where fly-by-wire kept a small plane from (large plane?) crashing when the pilot was hurt in a collision with a flock of birds? How about the people saved every day by airbags and anti-lock brakes? I know that the risks forum is intended to help us see and understand the risks, but many in the media view this forum as well, and perhaps we should consider the risks of only discussing failures and ignoring successes.

So, this whole thing was inspired by the British story about BA incidents. I have been in a 747-400 flying from DC to Heathrow (it starts in Pittsburgh) several times, and once we were told after a very smooth landing on a fairly poor landing condition day, that the computer have made the landing for us. I was pleased to know that I was an unwitting part of the great experiment, butthe landing was far smoother than most pilot landings in similar conditions, so I should feel pretty good about it.

The point is that the reason we don't have enough experts to do QA is that we don't teach that stuf in schools, we punish those who follow that line (as a society), and not enough executives lose their children in these incidents to

cause them to care about it. After all, we can't even detect a bomb on a 747 flying out of the most security conscious airport in the world (Heathrow - commercial that is), so why do we think we can track down minor computer software bugs that don't even kill hundreds of people?

Well, that's enough space for now - I'll continue my ravings at a later date.

P.S. How can we expect these computer systems to work so well when the computer I use to talk to the network doesn't let me see the last line when I reach the end of a page, doesn't let me backspace past a line break, and doesn't automatically check for spelling errors before sending my mail out? And this is a computer operated by the NSA designed for multilevel secure operation. It obviously has some major integrity problems. Until we get computers past these problems, I doubt if we will be able to design a truly safe fly-by-wire system to control aircraft.

FC

### Ke: Yet more Software-in-the-Air scares [<u>RISKS-13.50</u>]

Pete Mellor <pm@cs.city.ac.uk> Mon, 18 May 92 14:30:04 BST

Simon Marshall drew our attention to an article on:

> the front page of the UK ``Sunday Telegraph'' May 17, 1992, a so-called > ``quality newspaper''.

This was rather useful, since the only Sunday paper I normally read is the ``Observer'' (a \*real\* quality newspaper :-).

I would like to make a few comments on the article itself and on Simon's comments.

The article states:

<> But leading computer experts are worried that there is no adequate way of <> testing the enormously complex software routinely used by the aircraft <> industry.

and Simon comments:

> Given the number of years these systems have been

> around, it worries me to think that these relatively simple systems fail at

> this frequency, while fly-by-wire, with its increased complexity and the

> increased reliance upon those systems for the safety of the aircraft, is now

> being applied to commercial aircraft.

So are the systems complex or simple?

It depends which on-board system we are talking about.

Fly-by-wire systems (according to my best information - the probability of an

outsider being allowed to see the source code are slightly less than the required maximum probability of failure of a critical avionics system, i.e., 10^-9. :-) are \*relatively\* simple. They accept an input vector of flight parameters, multiply it by a matrix whose elements represent the "flight control laws" in force at that moment, and output a vector of signals to the hydraulic actuators which move the flight control surfaces. They control the second-by-second behaviour of the aircraft, and they don't have to "remember" too much: in the event of a transient failure, it is usually acceptable to reset them by switching off and on (if you have time! :-).

On the other hand they \*are\* regarded as "critical" from a certification point of view: they possess modes of failure which can crash the 'plane.

Flight Management Systems, on the other hand, are (by any standards) horrendously complex. They not only include the function of the traditional autopilot, but can also guide the aircraft over its entire route, including performing an automatic landing. To do this, they can in some cases access a database of airport information and topographical details of the approach terrain, and can select the cheapest or fastest route.

However, they are \*not\* regarded as critical: the pilot can override them, and if you just happen to be a few miles off-course, it's not necessarily fatal.

> at least some of the "software errors" were within> auto-pilot control systems (it may be all, the article is not clear -

The incidents cited in the article all involve sudden unintended manouevres. They \*could\* be due to the FMS "telling" the FBW to do something stupid, but might conceivably arise within the FBW. (Where the under/over thrust conditions are concerned, bear in mind that the FBW must "talk to" the engine controller, these days almost invariably a Full-Authority Digital Engine Controller (FADEC), and that the software in the FADEC is a single point of failure, since there is no diversity of the software in the duplex channels of the FADEC.)

> maybe BA does not fly any fly-by-wire aircraft anyway, I don't know).

It operates some A320s. The aircraft in the three incidents described are all recent Boeings, which don't have quite the same degree of automation at the FBW level, but still have some.

> The third is that the software had "CAA approval", as if this is meant to
 > make us feel any better, and that it had been tested by BA themselves
 > (not the CAA),

A few facts about "CAA approval":

To start with, the regulations stipulate quantitative demonstration of reliability for \*systems\*, i.e., the manufacturer must convince the Airworthiness Authorities that an on-board system has the famous maximum probability of catastrophic failure of 10^-9 per flying hour. (For less serious failure modes, higher probabilities are allowed.)

For the \*software\* in those systems, however, NO FIGURE IS PLACED ON RELIABILITY. Instead, a \*process\* certification, rather than a \*product\* certification is employed: the manufacturer has to provide the Authority with documents which show that a "good job" has been done in developing the software. These include (for software in critical systems) test plans and reports, details of inspections carried out, summary of achievement (whatever that is), etc., etc. These procedures and the required documents are specified in a set of guidelines: ``Software Considerations in Airborne Systems and Equipment Certification'', referred to as RTCA/DO-178A.

In no case do these guidelines oblige the manufacturer to make available to the Authority either a machine-readable copy of the source code or object code. The question of the Authority (or anyone else) doing independent verification and validation (IV&V) therefore simply does not arise with the regulations as they stand.

> for "100 hours before entering service". This does not seem particularly > rigorous to me!

I disagree that this is "not particularly rigorous". It's pathetic! In fact, I suspect that a proof-reader failed to spot a missing zero or two here. The A320 systems were run on a ground simulator for a year before the first test flight, and run for a further year in flight and on simulators before service.

> The fourth came with the old call for qualifications for those working in> safety-critical software design; lack of suitably trained people.

What John Cullyer meant here was training in formal mathematical methods: the use of formal specification languages such as Z or VDM, together with mathematical proof of correctness as part of verification. He's right, except that the use of such methods does not guarantee perfect software. In fact, no method that we know of, and possibly no \*conceivable\* method, would ever enable us to claim the incredibly low failure probability required by the regulations, where software is concerned (which would have been the main message imparted by Bev Littlewood in his talk to the ACM).

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

#### Re: yet more software-in-the-air scares

Martyn Thomas <mct@praxis.co.uk> Mon, 18 May 92 15:47:51 +0100

The Sunday Telegraph report was based on an issue of British Airways' newsletter FlyWise, which seems to be a monthly safety awareness newsletter for BA pilots. This issue covered January, and more incidents were caused by software than by any other cause except ground handling (eg trucks colliding with parked aircraft, baggage handlers denting the hull).

The UK trade paper, Computer Weekly, is covering the story in this Thursday's

issue. BA have apparently told them that the faults in the 747-100 and -200 were the result of a maintenance upgrade to the FMS, and were not safety-critical.

So, do these incidents provide any reason for concern? Do they reveal process failures in software maintenance? Do they reveal failures in recertification? Will DO-178B help? Should all airlines make their safety-records available for statistical analysis, so that Bev Littlewood can predict \*next\* year's reliability figures? These are some of the questions which probably won't be found in next week's Sunday Telegraph.

### ✓ Conference on Computer Assurance REMINDER

Laura Ippolito <ippolito@swe.ncsl.nist.gov> Mon, 18 May 92 09:19:47 EDT

**Final Announcement** 

COMPASS '92 SEVENTH ANNUAL CONFERENCE ON COMPUTER ASSURANCE

Systems Integrity, Software Safety, and Process Security

June 15-18, 1992 Gaithersburg, Md.

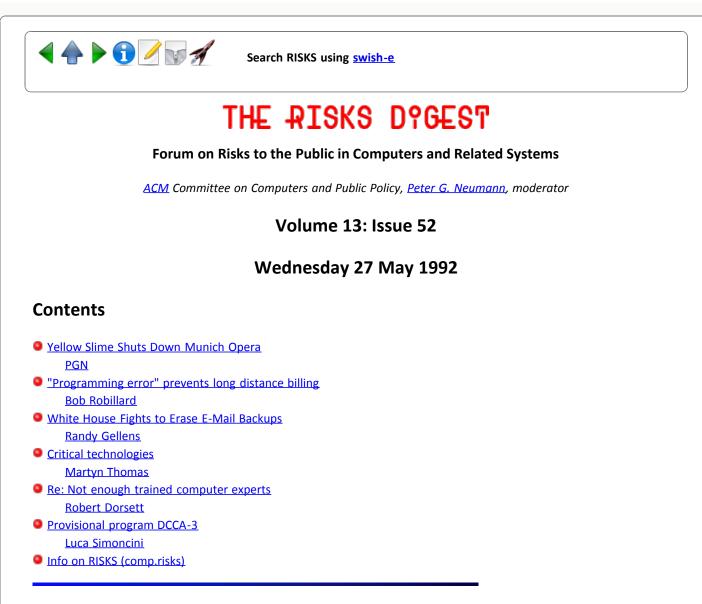
National Institute of Standards and Technology Technology Administration U.S. Department of Commerce

FOR MORE INFORMATION, SEE <u>RISKS-13.45</u>.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



### Yellow Slime Shuts Down Munich Opera

"Peter G. Neumann" <neumann@csl.sri.com> Wed, 27 May 92 15:08:05 PDT

The computer-controlled hydraulic system for the stage at the Munich Opera is a wonder of modern technology, controlling all rolling side stages, platforms, flats and panels. It is the ultimate play-by-wire system and for many explicitly programmed operas the show cannot go on without it. The problem is that the hydraulic fluid used in the new system (circulating in the old water pipes) is 50,000 liters of ecologically correct Quintolubric oil, made in the Netherlands. Unfortunately, it is biodegradable, and the bacteria left over from the old pipes love it. The result is a nasty yellow slime that multiplies fruitfully. The repertory has been trimmed dramatically, excluding those works that cannot be performed without it, and reducing some others to concert versions. Some performances have had to be halted in mid-scene, which requires cleaning all vents and filters. Audiences are upset. The cost to fix the problem (presumably to replace all the pipes and change the oil to something ecologically less sound) is estimated at \$24M. [Source: A NY Times article by John Rockwell, seen in the San Francisco Chronicle, 26 May 1992, p.E2]

[Could be messy if the Slime Disease gets into the Orchestra Pit. What productions would be appropriate under these circumstances? The Wizard of Ooze and the Yellow Bic Flowed? El AMARILLO cid? JAUNE of Arc? Der GELBrosenkavalier? The Russo-Japanese KI'IROI Ballet? Something by Norman Dello GIALLO? Certainly something Polish conducted ./

by Sir George ZOLTY? Pictures at an Exhibition by de KUNING in Indonesia? (In case you are puzzled, there is something yellow in every one of those, even ASFAR as the eye can see in the arabian desert.) I'm not yellow, but I thought I'd try out some multilingual puns on our multilingual readers in remote sites. I've been too kind in recent times, but not off color. PGN]

### "Programming error" prevents long distance billing

Bob Robillard <duke@ctt.bellcore.com> Fri, 22 May 92 12:35:23 EDT

THOUSANDS DIAL LONG-DISTANCE 'FREE' AS A COMPUTER GLITCH HANGS UP BELL Star Ledger:Newark-NJ, 22 May 1992, p.1

New Jersey Bell officials said yesterday that thousands of New Jersey Bell customers have been dialing long-distance between February 17 and April 27 without being billed for any of the calls. The situation, involving about two million calls, was blamed by New Jersey Bell on an internal programming error. The error affected 15 exchanges in the state and blanketed all direct-dialed calls made through AT&T. New Jersey Bell said the calls were registered and customers will eventually be back-billed, which could result in some large telephone bills. However, an AT&T spokesperson said customers could contact New Jersey Bell to "arrange a flexible billing arrangement so there is no financial hardship."

### White House Fights to Erase E-Mail Backups

<MPA15AB!RANDY@trenga.tredydev.unisys.com> 21 MAY 92 02:23

From a story by Paul Houston in the L.A. Times 20 May 1992:

Two days before President Bush took office, a researcher discovered that the new Administration planned to erase computer backup tapes containing thousands of messages sent by "electronic mail" [sic] throughout the White House of departing President Ronald Reagan.

The report alarmed groups representing historians and reporters, who for decades have been able to go to the National Archives and plow through the records of past Administrations, gaining valuable insight into how policies were formed and carried out.

The groups knew that some E-mail tapes already had been shown to carry incriminating messages between former National Security Advisor John M.

Poindexter and his aide, Oliver L. North, in the Iran-Contra scandal.

Fearing that much more treasure was about to vanish in this new electronic age, one group immediately filed suit and won a temporary order preserving many tapes. That ignited a far-reaching clash between researchers and the Bush Administration that is finally coming to a head Friday in federal court.

At stake is not only past tapes but present ones, which are being regularly erased before unknown numbers of messages can be printed out and saved for the National Archives.

"We are probably losing fascinating snatches of things that provide illumination and point you in new directions," laments Robert J. Donovon, who has written histories of former Presidents Harry S. Truman, Dwight D. Eisenhower and John F. Kennedy.

BACKGROUND: The federal Records Act requires that "all books, papers, maps, photographs, machine readable materials" dealing with government "policies, decisions, procedures, operations" be preserved for the National Archives.

In 1978, Congress made clear that the law applied to presidential records, including "electronic or mechanical recordations." The move blocked an attempt by former President Richard M. Nixon to control--and theoretically destroy--all tapes of conversations between him and his staff that had led to his resignation in the Watergate scandal.

When the Iran-Contra affair broke in 1987, investigators searched White House computer tapes for messages involving Poindexter, North and other White House aids. The aides thought they had erased the messages--but many were preserved on backup memory [sic] tapes.

One message that has been made public concerned a 1986 meeting at which North later admitted he lied to a group of congressmen about his support of the Nicaraguan Contras. A Poindexter aide reported by E-mail that "session was success," with North saying that he "gave no military advice" to the Contras. Poindexter forwarded the note to North, attaching an E-mail message of his own that said: "Well done."

ISSUES: "The Administration would call those two words a mere telephone message slip," and not a record that must be preserved, says Thomas Blanton, head of the National Security Archive, a research center that filed the pending suit. "But a historian would say those words give the whole picture of suborning testimony to Congress," he added.

The plaintiffs contend that the records preservation law clearly covers E-mail and that the head archivist has sole authority to determine which White House messages should be kept for posterity.

Justice Department attorneys respond that a White House manual--leaving it to aides to decide which E-mail should be printed out for safekeeping--is sufficient to comply with the law. Most of the messages are personal or trivial anyway, the attorneys contend.

The plaintiffs have asked U.S. District Judge Charles Richey to order the

Administration to turn over a large sampling of E-mail from the Reagan years so he can determine whether it--and by extension, much subsequent E-mail--should be preserved. Richey is expected to rule on the request Friday.

Randy Gellens randy%mpa15ab@trenga.tredydev.unisys.com [THIS BOUNCES FOR PGN] OR forward to postmaster@tredysvr.tredydev.unisys.com

#### Critical technologies

Martyn Thomas <mct@praxis.co.uk> Tue, 26 May 92 13:25:49 BST

Did I miss an earlier discussion of the March 1991 Report of the (US) National Critical Technologies Panel?

The software section makes depressing reading. Complexity is identified as the problem. CASE is identified as The Answer.

Under "Innovative Concepts", two are identified: rapid prototyping and modular software. (Perhaps this section got left in from a report a decade earlier, by mistake :-)

The impossibility of exhaustive testing is identified, yet testing is seen to be the answer! "Intensive efforts are underway to develop advanced testing tools that attempt to simulate the broadest possible set of conditions in which a program might operate. By reducing manual quality control requirements, these tools have the potential to greatly shorten the software development cycle and reduce development costs". By juxtaposition, this is set as the solution to "complex software cannot be exhaustively tested prior to release".

The section ends: "The central challenge in software development is automated code generation for sophisticated programs. The development of such tools is largely dependent upon artificial intelligence and other software-based technologies. ... ...".

The Risk? That someone might actually believe this stuff (although I concede that it seems unlikely).

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

### Ke: Not enough trained computer experts (FBCohen, <u>RISKS-13.51</u>)

Robert Dorsett <rdd@cactus.org> Thu, 21 May 92 02:32:37 CDT

I think there's a gigantic conceptual leap from the skepticism that people may have that an extant system (UNIX, in this case) can be reliably hacked to be something that it wasn't intended to be--secure--to extrapolating that to a broad notion that the ground-up design of a secure system is impossible. There are bases for both viewpoints: what actually happens has largely to do with the usual design trade-offs of features vs. functionality, and how much money the developing agency has to throw at the problem.

UNIX, with its historically anarchic functional development, and relatively simple OS, is a particularly bad example to be using. Yeah, there are lots of people at work developing secure UNIX, but I have doubts as to what's being done to the OS to pull it off. What they produce might run a shell, all the right software, and keep the bogiemen out, but the hackwork that's involved is pretty impressive. And hackwork tends to produce unforeseen effects: thus a never-ending cycle of fixes and hacks, to plug those unforeseen problems, in an ever-increasingly complex OS. It's no wonder people are skeptical.

Changing the fundamental emphasis of an aspect of an existing complex software system-- in this case, changing the "security" emphasis of UNIX to keeping errant Russians out, from keeping errant students or casual intruders out--is always more tricky than designing a system designed for a SPECIFIC emphasis from scratch.

#### > How come

>we never hear on the risks forum about any successes where the computer >security system saves people?

Why should we? We all know such systems exist. Or, at least, we hope they exist. I'm not willing to adjudge any complex program \*I\* write as "100% reliable." Notwithstanding logical or semantic errors, there are many ways in which a language can be misinterpreted or misimplemented by a given compiler. What's the cut-off point at which we can claim to judge a section of code "reliable"? 100,000 lines? 50,000 lines? 10 lines? Is an aggregate of such reliable segments in itself reliable? You tell me.

The \*problems\* occur where systems fail. It's way too easy to fall into a see-no-evil, hear-no-evil mindset, which seems to be precisely that which your advertisers--who you're complaining about--wish to propagate! It is my perception that the risks forum was intended \*precisely\* to offer an alternative to the widespread propagation of such attitudes in the industry. It serves an important purpose: to show people (including a great many students, not yet a part of the Real World) that the spec sheets can't always be believed; that sloppy, cheap design is all too often the order of the day; and that ideal, elegant solutions don't always get done right in the real world. We can read about elegant solutions in the journals, or have them ordained from some professor, any time.

>nuclear reactor stories where human error was detected and corrected by a >computer and saved us from a meltdown?

But isn't it so much more productive to concentrate on cases where such meltdowns were averted only by the last level of redundancy? And then debate why higher levels of redundancy failed? The possibility of the last level of redundancy failing NEXT time is so unacceptable that we can't possibly take time off and thank our lucky stars that we got it right, this time. Safety-critical systems require--DEMAND--INTENSE scrutiny and criticism.

>So, this whole thing was inspired by the British story about BA incidents.

But don't forget the two pilots in the cockpit, monitoring the instruments, \*waiting\* for the all-important comparator or autopilot annunciator to indicate a failure state, and ready, at the first sign of trouble, to CLICK IT OFF and go around. This being the sole emphasis of all their training: the determination of the point when a situation's going to hell, and what to do. An integral part of the \*safety\* checks of the system. THAT thought makes me comfortable, through a landing in weather I wouldn't be caught driving a car in. Unfortunately, though, I KNOW airline pilots who have too much faith in the automation, who expect it to do what they tell it to, who view it as an abstract entity that "does" things, and not merely a machine, a collection of parts, decisions, and compromises, a machine which, like all machines, can FAIL. They are trained like any other airline pilot, but can spend lifetimes with no fundamental problems, and get sloppy. Those pilots (and their passengers) DIE when they get too far behind the airplane, and rely on the computer to do their job. And lo and behold, the 747-400, which makes such wonderful landings, has a cockpit environment so secure, so amazing, that it's almost tailor-made to produce such attitudes.

But I know: the solution to sloppy pilots in automated cockpits is to increase the automation ("Hey, we can do it!"), to protect us from the pilots (ala A3[2-4]0 FBW), which, in turn, can produce even more isolated, insulated attitudes, thus producing even more fundamental mistakes. Ad nauseum.

Enjoy your next flight. :-)

>The point is that the reason we don't have enough experts to do QA is that we >don't teach that stuf in schools, we punish those who follow that line (as a >society),

I think you're mistaken. The sole reason that highly robust systems are not pursued, whether it be operating systems or retail-vertical software, is money. Cheap solutions that fit the customer or marketing specification, that don't break too often, are the order of the day. When companies are willing to spend more money on development--and research on methods, and training decent software engineers, and willing to postpone release a couple of years when the production process--which is an art, not a science, and not amenable to Harvard Business School management tactics--bogs down, AND society's willing to shoulder the extra costs all that will engender: THEN we'll have something to talk about. :-)

I can see what you're saying, but I don't think your position's very productive. Several times a year, RISKS sees "lighten up!" posts, but let's keep the name and charter of the digest in mind.

Perhaps we need a "USA Today" version of RISKS, a respite for when the gloom and doom becomes a bit much. :-)

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

# Provisional program DCCA-3 Luca Simoncini <simon@mv3500.iet.unipi.it> Mon, 25 May 92 16:14:41 -0100 DCCA-3 Preliminary Program, 3rd IFIP Working Conference on DEPENDABLE COMPUTING FOR CRITICAL APPLICATIONS Can We Rely on Computers? Splendid Hotel La Torre, Mondello (Palermo), Sicily, Italy, 14-16 September 1992 Organized by IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance In cooperation with IFIP Technical Committee 11 on Security and Protection in Information **Processing Systems** IEEE Computer Society Technical Committee on Fault-Tolerant Computing EWICS Technical Committee 7 on Systems Reliability, Safety and Security University of Pisa Istituto di Elaborazione dell'Informazione del CNR, Pisa Associazione Italiana per l'Informatica ed il Calcolo Automatico With the support of ITALTEL S.p.A, ANSALDO TRASPORTI, C.N.R. Comitato Nazionale Scienze e Tecnologie dell'Informazione, Comune e Provincia di Palermo **General Chair** L. Simoncini, University of Pisa, Italy Program co-Chairs C.E. Landwehr, Naval Research Laboratory, USA B. Randell, University of Newcastle upon Tyne, UK Local Arrangement and Publication Chair E. Ricciardi, IEI-CNR, Italy **Program Committee** J.A. Abraham, U of Texas, USA P. Bishop, National Power, UK A. Costes, LAAS-CNRS, France D. Craigen, Odyssey Research, Canada K. Dittrich, U of Zurich, Switzerland H. Ihara, Hitachi, Japan R.K. Iyer, U of Illinois, USA J.P. Kelly, U of California, USA R. Kemmerer, U of California, USA H. Kopetz, Technische U Wien, Austria J.H. Lala, CS Draper Lab, USA K. Levitt, U of California, USA B. Littlewood, City U, UK T. Lunt, SRI Int'l, USA J. Meyer, U of Michigan, USA M. Morganti, Italtel, Italy S. Natkin, CNAM, France J-J. Quisquater, Philips, Belgium R.D. Schlichting, U of Arizona, USA

F.B. Schneider, Cornell U, USA D. Siewiorek, Carnegie-Mellon U, USA L. Strigini, IEI-CNR, Italy I. Sutherland, ORA, USA W.M. Turski, Warsaw U, Poland Ex Officio J-C. Laprie, LAAS-CNRS, France, IFIP WG 10.4 Chair

This is the third Working Conference on this topic, following the successful conferences held in August, 1989, at Santa Barbara (USA) and in February, 1991, at Tucson (USA). As evidenced by papers that were presented and discussed at those meetings, critical applications of computing systems are concerned with differing service properties, relating to both the nature of proper service and the system's ability to deliver it. These include thresholds of performance and real-time responsiveness that demark loss of proper service (failure), continuity of proper service, ability to avoid catastrophic failures, and prevention of deliberate privacy intrusions.

The notion of dependability, defined as the trustworthiness of computer service such that reliance can justifiably be placed on this service, enables these various concerns to be subsumed within a single conceptual framework. Dependability thus includes as special cases such attributes as reliability, availability, safety, and security. In keeping with the goals of the previous conferences, the aim of this meeting is to encourage further integration of theory, techniques, and tools for specifying, designing, implementing, assessing, validating, operating, and maintaining computer systems that are dependable in the broad sense. Of particular, but not exclusive interest, are presentations that address combinations of dependability attributes, e.g. safety and security, through studies of either a theoretical or an applied nature.

As a Working Conference, the program has been designed in order to promote the exchange of ideas by extensive discussions. All the paper sessions will end with a 30 minute discussion period on the topics dealt with in the session. In addition to the paper sessions, three panel sessions have been organized. The first, entitled "Safe Vehicle-Highway Systems" will explore safety requirements, design methods and validation techniques for computing and communication subsystems associated with intelligent vehicle-highway systems. The second, entitled "Malicious and Inadvertent Human Operator Faults" will explore current and proposed techniques for detecting and countering faults introduced by the human operator. The third, entitled "Security Issues in Intelligent Networks" will deal with privacy problems related to the delivery of intelligent network services and related customer control, along with network security problems mostly related to open network provisioning.

Advance registration as well as hotel reservation is required. No on-site registration will be available.

Sunday September 13 Welcome Reception (7.00 - 10.00 p.m.), Hotel La Torre

Monday September 14 Opening Remarks (8.30 a.m.) L. Simoncini, General Chair

C.E. Landwehr, B. Randell, Program Co-Chairs Session 1: Functional Testing (9.00 a.m) On Functional Statistical Testing Designed from Software Behavior Models P. Thevenod-Fosse, H. Waeselynck (LAAS-CNRS, France) Functional Test Case Generation for Real-Time Systems D. Mandrioli, A. Morzenti (Politecnico di Milano, Italy), S. Morasca (University of Maryland, USA) Break (10.30 a.m.) Session 2: Specification and Verification of Fault Tolerance (11.00 a.m.) Design for Dependability J. Nordahl (Technical University of Denmark, Denmark) Tracing Fault Tolerance H. Schepers (Eindhoven University of Technology, The Netherlands) Lunch (12.30 p.m.) Session 3: Dependability and Performance (2.00 p.m) Evaluation of Fault-Tolerant Software: A Performability Modeling Approach A.T.Tai, A. Avizienis (University of California at Los Angeles, USA) Performance Analysis of Rollback Recovery in Process Control Systems A. Ranganathan, S.J.Upadhyaya (State University of New York at Buffalo, USA) On the Transient Analysis of Stiff Markov Chains J. Dunkel, H. Stahl (Universitat Dortmund, Germany) Break (4.00 p.m.) Panel Session 1: Safe Vehicle-Highway Systems (4.30 p.m.) Moderators: A. Costes (LAAS-CNRS, France), J.F. Meyer (University of Michigan, USA) **Tuesday September 15** Session 4: Application of Formal Methods (9.00 a.m) Formal Techniques for Synchronized Fault-Tolerant Systems B.L. Di Vito (Vigyan Inc., USA), R.W. Butler (NASA Langley Research Center, USA) Compiler Correctness and Input/Output P. Curzon (University of Cambridge, U.K.) Break (10.30 a.m.) Session 5: Online Error Detection (11.00 a.m.) Control Flow Checking In Object-Based Distributed Systems N.A. Kanawati, G.A. Kanawati, J.A. Abraham (University of Texas at Austin, USA) Time Behavior Monitoring as an Error Detection Mechanism H. Madeira, P. Furtado, J.G. Silva (University of Coimbra, Portugal) Lunch (12.30 p.m.) Session 6: Safety-Critical Industrial Systems (2.00 p.m) A "Strongly-Fail-Safe Majority Voted Output" Circuit used for Designing

Dependable Computer Systems

S. Noraz, M. Prunier (Merlin Gerin Company, France)

ACC: Dependable Computing for Railway Control Systems G. Mongardi (Ansaldo Trasporti, Italy)

Break (3.30 p.m.)

Panel Session 2: Malicious and Inadvertent Human Operator Faults (4.00 p.m.) Moderators: J.C. Laprie (LAAS-CNRS, France), T. Lunt (SRI International, USA)

Banquet (8.00 p.m.)

Wednesday September 16

Session 7: Experimantal Evaluation (9.00 a.m)

A Hybrid Monitor Assisted Fault Injection Environment

L.T. Young, R.K. Iyer (University of Illinois at Urbana-Champaign, USA)

Space/Time Overhead Analysis and Experiments with Fault-Tolerant Techniques L.A. Laranjeira, M. Malek, R. Jenevein (University of Texas at Austin, USA)

Break (10.30 a.m.)

Panel Session 3: Security Issues in Intelligent Networks (11.00 a.m.) Moderator: M. Morganti (Italtel S.p.A., Italy)

Lunch (12.30 p.m.)

Session 8: Protocols for Dependability (2.00 p.m)
Primary-Backup Protocols: Lower Bounds and Optimal Implementation
N. Budhiraja, K. Marzullo, F.B. Schneider, S. Toueg (Cornell University, USA)
A Linguistic Framework for Dynamic Composition of Fault-Tolerance Protocols
G. Agha, S. Frolund, R. Panwar, D. Sturman (University of Illinois at Urbana-Champaign, USA)
Using Two-Phase Commit for Crash Recovery in Multilevel Secure
Distributed Database Management Systems
S. Jajodia, C.D. McCollum (The Mitre Corporation, USA)

Conclusions (4.00 p.m.)

LOCATION: Splendid Hotel La Torre, Via Piano Gallo 11, Mondello, Palermo, Sicily, Italy Tel.: + 39 91 450222 ( or +39 91 450312) Fax: +39 91 450033.

HOW TO REACH MONDELLO: There are direct flights to Palermo from Paris, Munich, Rome, Milan and Pisa. From Palermo Airport take either a taxi to the Hotel or take the shuttle bus to the City Terminal in central Palermo, from where buses are available to reach the Hotel in Mondello.

SOCIAL EVENTS AND ARRANGEMENTS: During the Conference, the following events have been organized for participants and accompanying persons: \* SUNDAY, SEPTEMBER 13 (7.00 p.m.): Participants are invited to a Welcome Reception at the Hotel La Torre. \* TUESDAY, SEPTEMBER 15 (8.00 p.m.): The Banquet is kindly offered by APT Azienda Provinciale per il Turismo, Palermo. Buses will take the participants to the Banquet and then back to the Hotels. The price for Accompanying persons wishing to attend the Banquet is It. Lire 80000.

LUNCH: Lunches will be served at the Hotel La Torre. The price per lunch for Accompanying persons is It. Lire 35000.

TELEPHONE AND FAX MESSAGE: Participants may receive messages during the Symposium at the Hotel La Torre (see LOCATION).

CONTACT ADDRESS: For any information write to:

Ettore Ricciardi: IEI-CNR, Via Santa Maria, 46, 56126 Pisa, Italy Telex 590305 IEICNR I Fax + 39-50-554342 E-mail SIMON@ICNUCEVM.CNUCE.CNR.IT

DCCA-3, September 14-16, 1992

**REGISTRATION FORM** 

Surname Name Affiliation Address City State: Zip Tel.: Fax:

E- mail.

**REGISTRATION FEES** 

PRE-REGISTRATION IS REQUIRED. NO ON-SITE REGISTRATION

Before July 15, 1992: Lit. 380,000 Before August 15, 1992: Lit. 450,000

PAYMENT AMOUNT OF LIT.

.....

I enclose an International Bank cheque for the total amount indicated above.

I enclose photocopy of a bank transfer order (bonifico)

payable to: DCCA-3 Ettore Ricciardi, Bank Account n. 13761 Banca Popolare di Novara Ag. 1, Via S. Francesco,54- Pisa

Send in an envelope to: Ettore Ricciardi, IEI-CNR, Via Santa Maria, 46, 56126 Pisa, Italy

3rd IFIP Working Conference on Dependable Computing for Critical Applications DCCA-3

September 14-16, 1992

HOTEL RESERVATION FORM Surname: Name Affiliation Address

City						
City State	Zin					
Tel.:	Zip Fax.					
Tel	rax.					
Accompa	anied by (surname and name)					
I wish to	share a double room with					
Date of						
	DepartureTot					
Nights						
-						
Please re	eturn this form					
before Ju	before July 31, 1992 to: Ettore Ricciardi, IEI-CNR, Via Santa Maria, 46					
56126 Pi	56126 Pisa, Italy					
No depo	sit is required. The Hotel bill will be settled directly with the Hotel.					
Major cr	edit cards are accepted. A limited block of rooms has been reserved					
for partion	cipants to the Conference. Participants, whose Hotel Reservation Form					
arrive af	ter July 31, 1992, may have to be accomodated in nearby Hotels. EARLY					
HOTEL R	ESERVATION IS STRONGLY SUGGESTED. THE RESERVATIONS WILL BE PROCESSED IN					
STRICLY	FIRST ARRIVED FIRST SERVED WAY. Extension of the stay is possible at					
the same	e cost conditions.					
3rd IFIP	Working Conference on Dependable					
Computi	ng for Critical Applications DCCA-3					
Septemb	er 14-16, 1992					
ACCOM	AODATION:					
Single						
Lit. 1030	00					
no						
Double						
Lit. 1560	00					
no						
Triple						
Lit. 2020	00					
no						
Double a	is Single					
Lit. 1200						
no						
Please m	ark the accommodation you wish to reserve.					
N.B. *Dricos i	adicated are per including breakfast, convice charges taxes and VAT.					
	ndicated are per, including breakfast, service charges,taxes and VAT;					
	ooms have private shower or bath; ingle rooms are no longer available, double rooms for single use will					
be reser						
-	redit cards are accepted; remitted will be refunded, minus one day room cost, if written					
	on of cancellation arrives before September 1, 1992. Thereafter no vill be permitted;					
	-					
пе по	tel Management must be informed of changes to arrival time; rooms will					
1/0:1/12	52 html[2011_06_11_00.11.22]					



Nancy Leveson <leveson@cs.UMD.EDU> Thu, 28 May 92 06:29:42 -0400

(forwarded from Marty Kaszubowski)

In this week's Aviation Week and Space magazine, there is an article entitled

"Mission Control Saves Intelsat Rescue from Software, Checklist Problems." In the article it is stated that:

Analysis of the problem showed that it occurred when IBM, with NASA approval, made pre-launch changes in rendezvous software. ``It didn't work exactly the way they thought it would work,'' [launch director] Hale said.

The problem not only threatened the rendezvous, but also raised questions about the entire shuttle guidance and control software. ... ``We were concerned about the safety of all the other software on the orbiter -- if the computers don't work, nothing on the orbiter works."

# M The Thin Edge of the Wedge?

BARRY JOHNSON <WB15471@ibrdvax1.bitnet> Thu, 28 May 92 18:18:00 EDT

The Town of Vienna is a small bedroom-community enclave of about 15,000 people in the northern Virginian suburban overflow of Washington DC. Although dependent on the surrounding Fairfax County for many services (most notably schools and, for the sake of the second story, the cable franchise), Vienna does have its own police force.

Vienna is proposing to maintain a voluntary-entry next-of-kin database for all town residents, to be used only in the event of death or medical emergency. Contacting next-of-kin has been a serious problem in cases of recent fire victims. Opponents see this as a further incursion into privacy. [This paragraph starkly excerpted by PGN from "The Washington Post" FAIRFAX WEEKLY Section - May 21, 1992, `Next-of-Kin Plan Splits Vienna Residents', by By Whitney Redding - Washington Post Staff Writer. See also "The Connection", a local freebie weekly - May 6, 1992, `Police data base has some Vienna residents irked', by Darcy Nair, and a letter in the same issue. PGN]

The impression I get from this and other stuff that appeared was that a lot of it arose because a larger budget (several thousand dollars?) was originally requested to implement a "database"(? - and is it any coincidence the way this term seems to be bandied around?). My impression was that a proposal without the `computer' dimension (say, storing 3"-by-5" index cards in street address order) might not have caused such debate. Barry Johnson WB15471@IBRDVax1

## M The Federal Government and Civilian Encryption

## Larry Hunter <hunter@work.nlm.nih.gov> 28 May 92 11:24:06

The lead article in today's Government Computer News (5/25/92, v.11, n.11), entitled "NIST standing firm on digital signature," describes the efforts of the National Institute of Standards and Technology to defend its harshly criticized proposed standard, DSS. It contains some particularly important comments by the Chairman of the House Judiciary Committee, Jack Brooks, on executive branch actions regarding use of secure technology by the American public.

During the hearings, vendors and industry experts kept hammering at what they described as critical flaws in the DSS proposal. The Director of NIST, John Lyons, testified before the House Judiciary Subcommittee on Economic and Commercial Law that DSS is being established strictly for federal agency applications and should not impede the development of technology within the private sector. Under questioning, Lyons admitted that "Any standard improperly formulated can slow down and stifle technology."

At an earlier hearing, Assistant Comptroller General Milton Socolar (from the General Accounting Office) testified that DSS is weaker than a popular commercial signature verification product developed by RSA Data Security, Inc. of Redwood City, CA. He questioned whether requiring federal civilian agencies to use NIST's DSS, if it is less effective than commercial alternatives, would serve a useful purpose. He also said that the National Security Agency and the FBI pressured NIST into proposing a weak standard to ensure that NSA and FBI can crack it, and thereby forge digital signatures.

The chair of the House Judiciary Committee, Jack Brooks (D-Texas) agreed, stating that FBI Director William Sessions had told the subcommittee that the FBI is "against having security encryption devices that they could not break. They did not want any system that they could not have a key to," Brooks said. "They said it would give drug dealers, terrorists and buggers an advantage. That's what they said publicly, and there's no use dissenting on it."

[It certainly does give those buggers an advantage.... -Ih]

Brooks said Congress must be wary of White House efforts to grant intelligence agencies a greater role in civilian security matters.

[The rest of us should be vigilant, too.] Larry Lawrence Hunter, PhD., National Library of Medicine, Bldg. 38A, MS-54 Bethesda. MD 20894 (301) 496-9300 (301) 496-0673 (fax) hunter@nlm.nih.gov

## 🗡 White House records

<kittlitz@osf.org> Wed, 27 May 92 20:18:01 EDT

In RISKS-13.52, "White House Fights to Erase E-Mail Backups", it is noted that `In 1978, Congress made clear that the law applied to presidential records, including "electronic or mechanical recordations".' Does the executive branch use voice-mail? Will they have to re-program it so that old messages cannot be deleted; they just fade away to the archives? Think of all the telephone pranks (a la Bart Simpson) which might result. Spoofing of computer backups may also become more likely as their volume grows; will we need digital signatures (!) on the documents?

E. N. Kittlitz kittlitz@world.std.com kittlitz@osf.org (contracting at OSF, not representing their positions)

## Computer virus insurance

## John Mello <jmello@igc.org> Fri, 29 May 92 12:32:10 PDT

Followers of the Risks conference aren't the only ones worried about computer risks. So's your friendly neighborhood insurance agent. Several insurers have launched programs to protect businesses against computer mischief, namely computer viruses. And one, the Aetna Casualty and Surety Company of Hartford, Connecticut, has gone much further.

The major reason carriers aren't shying away from virus insurance is they don't expect to get whacked with significant losses. That certainly has been the experience of two companies that offer virus protection, the St. Paul Companies of St. Paul, Minnesota, and the Allstate Insurance Companies of Northbrook, Illinois. In 1991, St. Paul's losses were less than \$15,000. Allstate has had to pay off on its virus coverage but nothing in excess of \$5000. A typical small business computer policy from Allstate, which would automatically include virus insurance, would cover an exposure of \$25,000 to \$50,000 and have an average premium of \$250 to \$750.

An ambitious computer crime insurance program has been launched by Aetna. Called ACCENT (Aetna Coverage for Computer and Electronic Network Technology), the program, limited to financial institutions and service bureaus, includes protection against phone fraud, computer viruses, software piracy, and threats to set off "time-bomb" viruses, disclose security codes, and other forms of extortion.

## The risks of telling the truth about viruses

fc <FBCohen@DOCKMASTER.NCSC.MIL> Sat, 30 May 92 09:39 EDT

I probably shouldn't be writing this entry until I have time to cool down about it, so FLAME-ON=> ISPNews just published a tiny piece derived from an article I wrote them on benevolent viruses, and left my name attached. I think I will sue for liable and slander. If you get a chance to read this piece, please realize that they mangled it to promote the protection business. The main point of the article (which was written before the Michelangelo scare but only published this week) was that benevolent viruses are possible and that only the computer security industry wants to claim they are not - and the reason is so they can scare you into paying them. The article had a counterpoint to each point of an abusive article written in a previous issue, but of course the counterpoints were all removed and replaced by a single sentence saying you should support good viruses. The claims that you could write safe viruses were included, but the reasons why were removed. The article it criticized was given great placement, but the counterarticle was placed in a hard to find area and given half the space of the original article it criticized.

If you get ISPNews, write to the editor and tell them that you know about the hatchet job they did on my article. Tell them that you no longer trust them to tell you about integrity protection in computers, since they obviously don't

have any integrity and care more about money than truth (they will probably agree with that one). Cancel your subscription, and pull your advertising! (just kidding)

The point of all this is not that they mangled my article - I am used to that but rather that there is a tremendous risk in an uncontrolled protection racket that goes by the name of "computer security". If I told you your house would burn down unless you paid me \$100/year, you would probably report me to the police (and wonder why I charged so little). If someone in the protection rackets tells you your computer will crash and you will lose all your data unless you pay them \$100/year, how is that any different? There's a finite probability your house will burn down, and there's a similar probability you will suffer damage at the hands (bytes) of a computer virus. If you think the person will burn down your house by lighting a fire, you should be aware that some computer virus defenders have sent copies of viruses out to their customers on demo disks (along with an order form for the cure).

I would like the FTC to look into truth in advertising in the computer security industry, but I can't convince them that there is any false advertising, since they seem to think that nobody could be fooled into thinking that Norton antivirus would actually protect them from all future viruses (old ad), or that central point caught ALL 150 viruses (that they knew about - I knew about a lot more).

Oh well - so much for now. FLAME-OFF...

## C-17 problems attributed to software diversity

David G. Novick <novick@cse.ogi.edu> Wed, 27 May 92 10:45 PDT

C-17 Program Faces Problems in Manufacturing, Software (Excerpted from Aviation Week & Space Technology, May 18, 1992, p. 31)

The C-17 [military aircraft] program encountered manufacturing problems in flight control surfaces and criticism by the General Accounting Office of software development last week. [...]

Reviewing the status of C-17 embedded computer systems, GAO said the program is "a good example of how not manage software development when procuring a major weapon system." The Air Force waived or ignored many Pentagon software standards and guidelines, gave Douglas Aircraft Co. control over software development, limited its own access to software information, and restricted its ability to require correction of problems, even after critical problems were evident, GAO said.

"In essence, the Air Force assumed that software was a low-risk part of the C-17 program and did little to either manage its development of to oversee the contractor's performance," GAO said. "Douglas (with the Air Force's concurrence) to a number of shortcuts that have substantially increased the risk of not successfully completing software development and testing and may result in substantially higher software maintenance costs with the C-17 is

eventually fielded.

[The first C-17 in 9/91 had all safety software but only 34% of avionics software. The complete software is supposed to be provided with the second aircraft in 6/92. The GAO lays the blame on proliferation of languages in the project. The systems were supposed to have been written in Ada, but Douglas had been working in JOVIAL. Further,]

... Douglas had trouble finding subcontractors who would use JOVIAL, however, and the Air Force "allowed the subcontractors to develop software in whatever language they chose." As a result there are six languages, four of them using existing as well as newly developed code and one of them proprietary to General Electric Co. Many subsystems contain more than one language. There are three in the flight control computer, for example.

[The Air Force now plans to convert all this code to Ada, which may be difficult because of inadequate documentation.]

David G. Novick, Computer Science and Engineering, Oregon Graduate Institute of Science and Technology, 19600 N.W. Von Neumann Drive Beaverton, OR 97006-1999

## C-17 story, Chmn. McDonnell's reply

"GVA::MLC" <MLC@IBERIA.CCA.CR.ROCKWELL.COM> 29 May 92 06:39:00 PST

Chairman McDonnell's reply to some of the C-17 criticisms follows. This was sent to me from my brother at McDonnell-Douglas. Neither one of us is/was involved in the C-17 work. Michael Cook [Don't reply to Michael!]

\_\_\_\_\_

C-17 - The Real Story

To All Teammates: May 13, 1992

The chorus of critics has been out in force lately. Their target: our C-17 program. These critics continue to focus on outdated, unsubstantiated allegations, and in some cases flat untruths about the C-17. They also echo the groundless charges that we were "bailed out" of financial difficulty by the government. I'm angry about this partial, slanted, misleading reporting, and you should be too. You deserve to hear the real story.

Let's begin with the C-17 wings. The critics have focused on the Drivmatic machine, saying the rivets it installs do not fully expand all of the time. Here are the facts. First, the C-17 wing is designed to last 60,000 hours, or twice as long as the required 30,000-hour life of the airframe. Second, fully expanded rivets add to that 60,000 hours. Those that do not fully expand do not detract from wing life. Beyond that, we have improved the processes and the machines. Our own internal investigations and those of Department of Defense agencies and the FBI found no fraud or wrongdoing. The bottom line: There is no safety of flight issue. There was no cover-up. The wings exceed contract requirements.

A network television reporter claimed the Drivmatic machines caused fuel leaks in the wing. Here are the facts. None of the leaks occurred around fasteners installed by the Drivmatic machines. We told the reporter that. We explained in detail to him where the leaks were found. In addition, we described the leak rate, which was less than one drop per minute; we told him we found that out of position work had caused the problem; we told him we had developed a new sealing process; and we told him we had taken the precaution of doing a reinspection of all wing sealing in every aircraft on the production line. He chose not to report the facts.

Some critics say we fired the employees who reported and investigated the Drivmatic issue. Here are the facts. Both individuals were fully involved in our investigation of the issue. The individual who reported the issue was given a pay raise for his role, but then just stopped showing up for work. After a period of months, we fired him just as we would any other employee who failed to show up for work for extended periods. The second individual, an internal investigator, had been identified as a part of a reduction in force decision a month before the investigation started. He was ultimately let go as part of our overall reductions, and not for any reason related to the investigation.

Other critics say problems are showing up in the C-17 flaps. Here are the facts. Early ground testing showed greater pressure on the flaps than had been anticipated in design. The flaps were redesigned and new flaps were made available for the first production aircraft. In actual flight, it turns out the pressures were much less than the ground testing had predicted. Result - the present flap exceeds contract specs. Flight testing also shows higher temperatures than anticipated in one area of the flap. We made a relatively simple change to more temperature-resistant materials. Those who attempt to judge a program solely by problems found and fixed during tests seem to ignore that one purpose of a test program is to do just that. The fact is that these incidents are a test program success, not a failure.

Still others question our candor on the C-17. Here are the facts. We keep our customers fully informed. We are consistently on the record with the facts concerning our problem areas as well as successes. Most recently we joined with the United States Air Force and the Grumman Corporation in announcing an inspection program to detect possible flaws in composite materials provided by Grumman.

Some alarmists claim the taxpayers will pay billions in contract ceiling overruns. Here are the facts. This is a fixed-price type contract for development and initial production of C-17. We believe the government is responsible for at least some of the cost growth, and we are submitting claims for those costs. Once our claims are resolved, we pay any difference - not the taxpayer. As for those who project costs greater than \$8 and even \$9 billion, with more than 90% of the work done, we believe our estimate of \$7.39 billion is correct.

Finally the bailout allegation. We didn't ask for a bailout, and we didn't get one. The facts are simple. We do the work, we submit bills, and then we get paid.

And now to conclude the real story. We are continuing to improve. We are building each new C-17 with far fewer labor hours than the previous aircraft. We are reducing rework. We are flying a rigorous test program - more than 200 hours so far - and passing with top grades. And in the final analysis, we will silence the chorus of critics with our successes.

John F. McDonnell, Chairman and Chief Executive Officer

## 🗡 SDI Costs

<[anonymous]> Thu, 28 May 92 9:06:36 PDT

Report Questions SDI Estimates

WASHINGTON (AP)

Deploying an antimissile defense system will cost \$37 billion over five years, about \$10 billion more than the Bush administration estimates, a congressional report said Wednesday.

The Congressional Budget Office said costs for the Strategic Defense Initiative from fiscal 1994 to fiscal 1997 would be about \$8 billion a year. President Bush has requested \$5.4 billion for the system in the fiscal year beginning Oct. 1.

SDI Director Henry Cooper has said building a system of defenses would cost \$25 billion. The government has already spent about \$29 billion on the program commonly known as Star Wars.

The CBO based its report on administration figures for research, development and procurement of a single-site defense at Grand Forks, N.D., by late 1997.

The program would include either ground-based or space-based sensors to detect incoming missiles, interceptors and a controlling command system.

Last year, leading defense Democrats such as Sen. Sam Nunn, D-Ga., and Rep. Les Aspin, D-Wis., joined congressional Republicans in backing the Missile Defense Act, which set a new goal for the program.

The law directs the administration to deploy an SDI system by 1996 or when the technology allows that would comply with the U.S.-Soviet Anti-Ballistic Missile treaty of 1972.

The CBO calculated the cost of alternatives to the administration's SDI plan, including a system favored by Nunn, Aspin and several Republicans. That system would cost \$31 billion with an average annual budget of \$7 billion.

The system would be deployed at a single site by 1997 and would include an additional system of sensors known as the ground-based surveillance and tracking system. It also would spend less money on space-based interceptors such as Brilliant Pebbles.

The House Armed Services Committee, in its version of the fiscal 1993 military budget, approved \$4.3 billion for SDI, cutting about \$1 billion from Bush's request. The panel eliminated all funds for space-based interceptors.

The CBO report acknowledges that its estimates "do not attempt to account for cost increases that might occur during development of a technically challenging project such as missile defense."

In August 1988, the CBO examined the cost growth of more proven weapons such as missiles, helicopters, tanks and fighter planes. It found that concurrent work on each program resulted in a cost growth of 193 percent to 288 percent. Rep. Charles Bennett, D-Fla., one of four House members to request the report, said the CBO cost estimates combined with recent comments from Cooper that deploying an SDI system by 1997 is a major challenge, creates a "recipe for cost overruns and operational effectiveness problems. With real defense assets being scrapped for budgetary reasons, it is hard to justify big expenditures for a questionable concept like SDI," Bennett said.

Aspin, Rep. Ron Dellums, D-Calif., and Rep. John Spratt, D-S.C., also asked for the SDI report.

## Kisks of SDI?

neumann@csl.sri.com <Peter G. Neumann> Fri, 29 May 92 15:09:22 PDT

An AP item in the San Francisco Chronicle on 26 May 1992, p.A3 noted that at least \$7.7 billion (out of a total investment of \$29B) in Star Wars projects "never got off the ground", being "cast aside as unneeded, unworkable, or unaffordable". These included the following:

- \* A surveillance satellite to detect and track hostile missiles. \$1B. Dead.
- \* A ground-based laser to zap missiles in flight by bouncing laser beams off relay and "fighting" mirrors stationed in space. At least \$1.2B. Mothballed.
- \* A Nuclear bomb-powered X-ray laser and other "nuclear-directed energy" weapons in space. At least \$1.8B. Dead.
- \* A pop-up "probe" to help interceptors distinguish warheads from decoys. At least \$.5B. To be mothballed in 1993, but until last year deemed `essential'.
- \* A guided rocket to intercept hostile missiles inside or outside the atmosphere. \$623M. Mothballed.

## New CPSR List Server

Ronni Rosenberg <ronni@ksr.com> Wed, 27 May 92 13:32:44 EDT

Computer Professionals for Social Responsibility (CPSR) has set up a list server to (1) archive CPSR-related materials and make them available on request, and (2) disseminate relatively official, short, CPSR-related announcements (e.g., press releases, conference announcements, and project updates). It is accessible via Internet and Bitnet e-mail. Mail traffic will be light; the list is set up so that only the CPSR Board and staff can post to it. Because it is self-subscribing, it easily makes material available to a wide audience.

We encourage you to subscribe to the list server and publicize it widely.

To subscribe, send mail to:

listserv@gwuvm.gwu.edu (Internet) OR listserv@gwuvm (Bitnet)

Your message needs to contain only one line:

subscribe cpsr

## Call for Papers, IFIP/Sec '93

"Dr. Harold Joseph Highland, FICS" <Highland@DOCKMASTER.NCSC.MIL> Thu, 21 May 92 09:50 EDT

ANNOUNCEMENT AND CALL FOR PAPERS IFIP/Sec '93 in Toronto -- May 12-14,1993

IFIP/Sec'93, the Ninth International Computer Security Symposium and Exhibition, is part of a series of international conferences devoted to advances in data, computer and communications security management, planning and control. It will be held May 12-14, 1993 in Toronto Canada.

This international conference, with the theme "Discovering Tomorrow", will encompass developments in both theory and practice and is intended for computer security researchers, managers, advisors, EDP auditors from government and industry, as well as other information technology professionals interested in computer security.

The purpose of the 1993 International Federation for Information Processing Security Conference [IFIP/Sec'93] is to provide a forum for the interchange of ideas, research results, and development activities and applications amongst academicians and practitioners in the information, computer and systems sciences. IFIP/Sec'93 will consists of advanced seminars, tutorials, open forums, distinguished keynote speakers and the presentation of high-quality accepted papers. It is hoped that there will be a high degree of interaction and discussion amongst conference participants, as a workshop-like setting is to be promoted.

The upcoming conference, IFIP/Sec'93, is jointly organized by IFIP/TC 11, the Canadian Information Processing Society [CIPS] and the Toronto Chapter of the Information Systems Security Association [ISSA].

#### **Call for Papers**

Papers are invited in the areas shown and may be theoretical, conceptual, tutorial or descriptive in nature. Submitted papers will be referred, and those presented at the Conference will be included in the Conference proceedings. Submissions must not have been previously published and must be the original work of the author(s). Possible topics of submissions include, but are not restricted to:

Auditing the Small Systems Environment Auditing Workstations PC and Microcomputer Security Security and Control of LANs and WANs OSI Security and Management Electronic Data Interchange (EDI) Security Management and Control of Cryptographic Systems Security in High Performance Transaction Systems Data Security in Developing Countries Software Property Rights Trans-border Data Flow Database Security Risk Assessment and Management Legal Response to Computer Crime/Privacy Smart Cards for Information Systems Security Biometric Systems for Access Control Security and Privacy in Electronic Mail

#### **Refereeing Process**

All papers and panel proposals received by the submission deadline will be considered for presentation at the IFIP/Sec'93 in Toronto. To ensure acceptance of high-quality papers, each paper submitted will be blind refereed.

The papers presented will be included in the Conference preprint of the Conference Proceedings, copies of which will be provided to the Conference attendees. All the papers presented will also be included in Proceedings which will be published by Elsevier Science Publishers B.V. (North-Holland). Author(s) will assign copyright of the paper to IFIP. Additionally, one or more of the authors must present the paper at the conference. Presenters of papers are eligible for a reduced conference fee.

#### Instructions to Authors

Three (3) copies of the full paper, consisting of 22-26 double-spaced, typewritten pages, including diagrams (approximately 5,000 words), must be received no later than October 1, 1992. Diskettes and electronically transmitted papers will NOT be accepted. Papers must be sent to the Program Committee Co-Chairman.

Each paper must have a title page which includes the title of the paper, full name of all author(s) and their complete address(es), including affiliation(s), telephone number(s) and fax number(s). To facilitate the blind review process, the author's particulars should appear only on the separate title page.

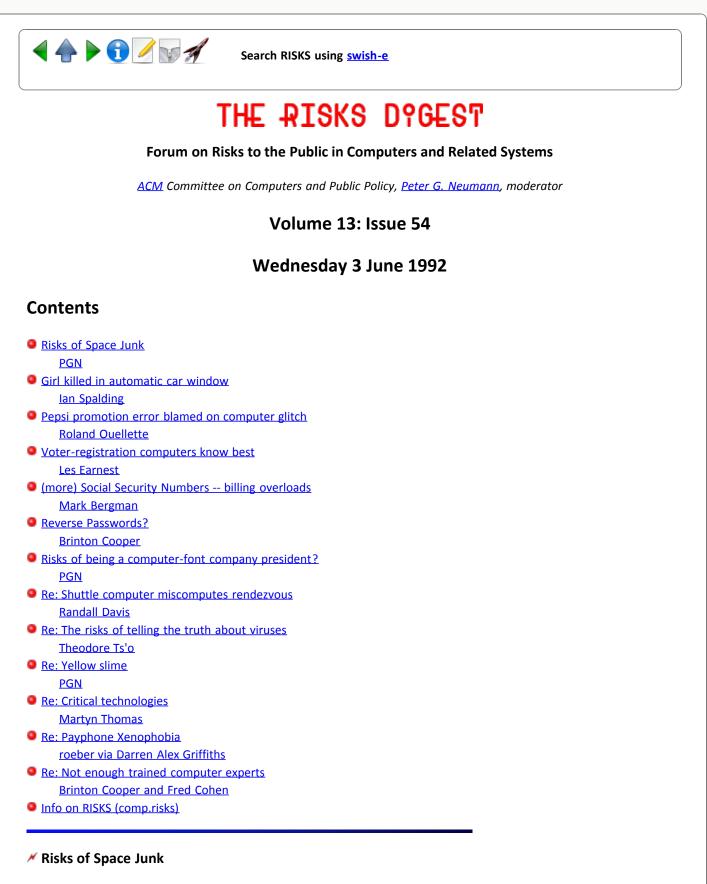
The language of the Conference is English.

The first page of the manuscript should include the title and a 300 word abstract of the paper. Abstracts may be submitted to the Program Committee if guidance and indication of appropriate content is required.

Full papers must be received by:October 1, 1992Conference dates:May 12-14, 1993

Papers Submission Mr. Graham Dougall, IFIP/Sec '93 -- Program Committee Co-Chairman c/o Concord-Eracom Computer Ltd, 7370 Bramalea Road, Unit 18 Mississauga, Ontario Canada L5S 1N6
Registration and Other Enquiries
Those interested in additional information about the upcoming conference on May 12-14, 1993 should communicate with the Organizing Committee's Chairman. Mr. Dave Batchelor, IFIP/Sec '93 -- Organizing Committee Chairman c/o Concord-Eracom Computer Ltd, 7370 Bramalea Road, Unit 18 Mississauga, Ontario Canada L5S 1N6 FAX: (416) 672-0017
FOR IMMEDIATE HELP: Highland@dockmaster.ncsc.mil

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Tue, 2 Jun 92 18:55:39 PDT

"Space Junk May Threaten NASA (Space) Station"

A NY Times item seen in the San Francisco Chronicle (2 Jun 1992, p.A7) quotes the current issue of Space News, which reports that NASA experts have adopted new calculations on collisions between space junk and the space station, which suggest that the risks are much greater than previously thought. They estimate that there may be 30,000 pieces of debris, mostly from old spacecraft that have broken up. Adding protective shielding might significantly raise the cost, already estimated at \$30B to \$40B.

## ✓ Girl killed in automatic car window

Ian Spalding <ins@praxis.co.uk> Tue, 2 Jun 92 14:10:58 BST

The following appeared in `The Guardian', on 2 Jun 1992:

Fiat, makers of the Tipo in which two-year-old Lucinda Richardson died when an automatic window shut, said last night that one of the front doors has to be open and the switch continuously depressed to close a front window when the ignition key was removed.

Lucinda's father, Douglas, said she must have stepped on the switch while playing in the car.

A statement issued by Fiat's UK headquarters at Slough, Berkshire, said: "The system ... meets German standards, to which all manufacturers conform." [..]

Labour called on the Government to issue immediate regulations to compel car maufacturers to fit vehicles with safety devices which automatically cut out motors on electric windows as soon as pressure is applied. The Royal Society for the Prevetion of Accidents urged manufacturers to examine the design of electric window design.

I don't believe that this particular window system is computer controlled ..., but I do know that several of the quality cars on the market have many of their body functions, including windows, under control of a central processor.

Ian Spalding

### Pepsi promotion error blamed on computer glitch

Roland Ouellette <ouellette@tarkin.enet.dec.com> Wed, 3 Jun 92 10:46:59 EDT

[Roland called our attention to an item in The Wall Street Journal, 1-Jun-92, p. B6B, which I have abstracted as follows. PGN]

Computer Glitch - 500,000 Pepsi bottlecaps turn into "winners"

PepsiCo's Philippine bottling franchise has had a promotion with numbers

printed in the bottle cap. A winning number was supposed to pay off up to \$38,000. A "computer glitch" was blamed for "349" being announced as the winning number, even though that number appeared on 500,000 bottle caps. Several thousand people accepted PepsiCo's offer of \$19 to each "winner", but about 4,000 people are seeking governmental action for fraud.

[This might lead to a new tack in creative advertising -- planning ahead of time to have an effort backfire so as not to have to pay off, with the a priori intent of blaming it "on the computer". PGN]

## Voter-registration computers know best

Les Earnest <les@sail.stanford.edu> Tue, 2 Jun 92 15:03:02 -0700

Is anyone with a given name and date of birth who lives in the same county necessarily the same person? That is what the Santa Clara County (California) voter registration computer believes, as reported in today's San Jose Mercury News.

John P. Taylor, a San Jose patent lawyer, has voted in every election since 1979, but he didn't receive his voting materials in the mail this year even though his wife, two sons, and daughter did. On checking with the regristrar of voters he discovered that another John P. Taylor, who happened to have the same date of birth, had recently registered in nearby Sunnyvale -- both were born on Christmas 56 years ago. The computer "knew" that a person with the same name and date of birth was the same person and so treated the transaction as a change of address. The computer records showed different places of birth, but it apparently wasn't programmed to check that.

While county authorities scratched their heads over this improbable event and what to do about it, the disenfranchised John P. Taylor telephoned the other one and worked out a quick fix. It seems that their middle names are Paul and Phillip, so they agreed to re-register with their full names.

What do you think are the chances that this programming blunder will be fixed before it claims its next victim? In the meantime, voters with common last names might consider registering their full names in order to reduce the chances of being victimized by this kind of programming foolishness.

Les Earnest, 12769 Dianne Drive, Los Altos Hills, CA 94022 415 941-3984 Les@cs.Stanford.edu ... decwrl!cs.Stanford.edu!Les

## // (more) Social Security Numbers -- billing overloads

Mark Bergman <bergman@panix.com> Thu, 28 May 92 0:25:24 EDT

INDIANAPOLIS (AP) - Claudia Braun is only 9 months old, but already her credit rating is shot. Indiana University Medical Center computers show that the youthful Miss Braud has run up bills of more than \$3,000 for medical services -

including pregnancy tests and dental care. Since late last year, the baby and her parents, Jean and Thomas Braun, have received about 15 bills, all for services rendered to people they don't know. Each bill listed Claudia as the person responsible for ensuring it got paid.

"I'd love to see them take me to court and carry her into court and say, `Hi, this is Miss Claudia Braun," Thomas Braun said. "Its hilarious when you think about it. But it's getting to be an old joke," added Mrs. Braun, a registered nurse at Wishard Memorial Hospital.

Robert D. Wehling, associate director of fiscal affairs at the medical center, said the problem began when Claudia entered the world without a Social Security number.

The university's computer program, which had just been installed, registered Claudia as 000-00-0000. Later, when other patients who didn't know their Social Security numbers were entered, they got 00-000-0000, too. The computer decided that all the patients with the zeros must be related, and put Claudia in charge of paying the bills. At last count, there were 37 patients linked to Claudia's account.

Medical center officials thought they had the Braun problem fixed in February and sent the family a letter of apology. But the computer then spit out seven more bills. New computer software was installed Tuesday that Wehling said should eliminate the problem. "We're sorry it happened," Wehling said. "This should not happen again."

Mark Bergman 718-855-9148 {cmcl2,uupsi,uunet,apple}!panix!bergman

## Keverse Passwords?

Brinton Cooper <abc@BRL.MIL> Wed, 3 Jun 92 10:05:52 EDT

>From the "Federal Employees News Digest," 18 May 1992:

An employee who forgot to type a two-character code in accessing a computer at work that then gave him unauthorized access to a check generating program should not have been disciplined for the mistake, the Merit Systems Protection Board has said.

The problem began when an Army depot switched certain information from a mainframe computer to mini-computers. When the employee tried to access his normal work-related files, he ran into problems and inadverently created a file listing banks and companies that were to get checks over one million dollars...The checks never were actually generated, however.

It goes on to report that the Army demoted the employee and that MSPB ordered him reinstated because the mistake was a "simple one" and because the employee had nothing to lose.

The RISK: Often, we've discussed the risks of not using proper passwords to prevent unauthorized access. This is the first time that I've seen a user required to supply a password in order that he NOT be granted access to files. This is quite a perverse risk!

Brint

## Kisks of being a computer-font company president?

"Peter G. Neumann" <neumann@csl.sri.com> Sun, 31 May 92 17:25:52 PDT

Most of you have read about last week's kidnapping of Charles Geschke, head of Adobe Systems, Inc., in Mountain View CA, and his successful rescue by the FBI after four days of captivity. We wish to express our appreciation for the way in which the rescue was carried out, and to send our best wishes to the Geschkes for some sort of return to a normal life.

In general, security (whether with respect to individuals, corporations, computers, or communications) is very difficult to ensure. In many cases the threats are not even perceived -- let alone defended against -- until they have flagrantly manifested themselves. Increased awareness of the incredible gamut of problems is vital. But the problems are inherently never completely solvable -- there are no guaranteed solutions. This is by itself a very important realization.

Technological solutions to security problems (in general) must be accepted as just one of many approaches. In the Geschke case, apparently the FBI planted transmitters in the package of ransom money. The kidnapper who picked up the money had a transmitter sniffer that detected some but not all of the planted transmitters. Even there the technology seems to escalate the use of countermeasures and countercountermeasures, as well as escalating the risks. PGN

## Ke: Shuttle computer miscomputes rendezvous (Sullivan, <u>RISKS-13.49</u>)

Randall Davis <davis@ai.mit.edu> Mon, 1 Jun 92 11:29:07 edt

The spacewalk was [...] delayed for 1 1/2 hours because Endeavour's on-board computer made a mistake in plotting the route needed to rendezvous with the satellite.

It is of course completely false. Endeavor's on-board computer might have gotten the wrong result because its programmers made a mistake, or perhaps the data entry folks made a mistake, or perhaps because its fabricators made a mistake, or even because its designers made a mistake.

The difference is not pedantry; it goes directly to the issue of what the risk is in computers. Saying the computer made a mistake encourages people to think that the machine errs like people, due to wandering attention, fatigue, etc.

One result of that in turn is less attention to the real culprit: programming, data entry, or fabrication, or design, or whatever else some human did wrong. A second result is the ability to shut off constructive demands for improvement by making it far too easy to offer the standard excuse: "It's just those goofy computers again <shrug>; there's not much we can do about them."

There's not much immediate personal impact from this particular application of course, but the identical issue arises all the time in response to ATMs, insurance claims, etc., etc., ad nauseum.

### Ke: The risks of telling the truth about viruses

Theodore Ts'o <tytso@ATHENA.MIT.EDU> Tue, 2 Jun 92 16:40:35 -0400

We've discussed this subject before on risks, but I don't believe that there is such a thing as a "benevolent virus". If I am a user, I don't want some new piece of software, which I normally don't run, to be automagically executed on my machine without my being informed about it, and given an option to veto it.

It all boils down to what your definition of "virus". My definition of "virus" is a piece of software which transmits itself from machine to machine without the knowledge or permission of either a user on the system or the system administrator of the machine. Using this definition, I do not believe there can be such a thing as a "benevolent virus", because I, as a system administrator or a user, want control over what I run on my machine. Perhaps I am running some special software that I know will break if my operating system gets upgraded --- I don't want a "OS Updating Virus" to go in and change my system without my permission. That's just wrong.

If you have some other, more broader definition of "virus", which includes the ability for the user or system administrator to veto or delay it --- I suggest you not use the term "virus". For one thing, the battle is lost. People think of viruses as bad (and I suspect most of them have a similar definition of virus as I presented). It's like the use of the word "hacker" --- at this point, it's practically hopeless to try to convince people that there is such a thing as a "good hacker"; the language has evolved to the point where the only definition of a "hacker" is a "system cracker"; the original definition of "super-competent programmer" has be long lost.

- Ted, (617) 253-8091

### Ke: Yellow slime (<u>RISKS-13.53</u>)

"Peter G. Neumann" <neumann@csl.sri.com> Wed, 3 Jun 92 8:29:33 PDT

Several people (for example, Martin Hofmann <hofmann@sap-ag.de>) asked me why that piece appeared in RISKS. My answer was something like this:

RISKS is by definition concerned with computers and related technology. The stage system is computer controlled, but the point is that even the most modern computerized installation can be brought to a halt by something seemingly unrelated to the computer! Usually it is people. This time it is a choice of hydraulic fluid and the decision to use the old pipes. Incidentally, Nigel Hall <N.F.Hall@newcastle.ac.uk> commented that "proper biodegrading hydraulic fluid, which looks like yellow slime, removes anything non-metalic in its path (especially automotive paintwork)" ...

### Ke: Critical technologies

Martyn Thomas <mct@praxis.co.uk> Tue, 2 Jun 92 9:17:35 BST

Several people have asked me for a reference for the March 1991 Report of the National Critical Technologies Panel, which I referred to in <u>Risks 13.52</u>.

It has no standard reference number. It is a report to the President of the USA and Congress, and required every two years "through the year 2000" (1990 Defence Authorisation Act [P L. 101-189] modifying the Natuional Science and Technology Policy, Organisation and Priorities Act of 1976).

The Panel's address is 1101 Wilson Boulevard, Suite 1500, Arlington, Virginia, 22209. The Chair is William D Phillips.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

### Ke: Payphone Xenophobia

Darren Alex Griffiths <dag@ossi.com> Mon, 1 Jun 1992 22:53:26 GMT

This is a post that I saw on comp.dcom.telecom. I think the risks are obvious (i.e., downloading a description of a lead slug).

roeber@vxcrna.cern.ch writes:

>Oh yes, I don't know why I didn't remember this immediately.

#### >

>Last year, at Telecom'91 here in Geneva, a company whose name I forget
>was showing a payphone that recognized coins based on a set of rules
>(weight or mass, size, etc.) programmed in a microprocessor. So its
>first advantage is that it can be used in many countries, and can even
>(if the owner wishes) take multiple currencies. The advantage they
>were really touting, though, was the ability to remotely call the
>phone, log in, and download new rules. This way when a country
>introduces a new coin (as Italy did a few years ago) or replaces a
>coin (as France did last year), one does not have to replace the
>phone, or even physically visit it.

>Frederick G. M. Roeber | CERN -- European Center for Nuclear Research>e-mail: roeber@cern.ch or roeber@caltech.edu | work: +41 22 767 31 80>r-mail: CERN/PPE, 1211 Geneva 23, Switzerland | home: +33 50 42 19 44

# Ke: Not enough trained computer experts (Marshall, <u>RISKS-13.50</u>)

Brinton Cooper <abc@BRL.MIL> Fri, 29 May 92 9:45:30 EDT

From: Brinton Cooper <cooper@dewey.udel.edu> fc <FBCohen@dockmaster> writes:

> Over the last several years, I have applied for positions in over 100
 > universities, and the universal response is that protection is not of interest
 > to the university community. This dispite the recent report from the US
 > National Research Council that calls for increased university research in the
 > field.

> You cannot find a single US university (and only a few outside the US) with
> more than 2 computer security experts on the same faculty. You also cannot
> find a university in the US where more than one person was hired with the prior
> knowledge that they have computer security interest (again I am talking about
> faculty positions). With the educators woefully ignorant, we can only expect
> the students to be equally ignorant.

We then conducted the following dialog; fc suggested that I submit it to Risks.

#### BRINT:

I'm interested in your comments about the paucity of university faculty who are knowledgable in computer security. The issue is an old one, but I've never fully come to grips with it.

Teaching a 3-rd year course in operating systems... I introduce concepts of "protection" in various units of the course, especially those involving memory sharing and file system design. Also, to facilitate handling of programming projects, I try to be sure that the students understand the unix file permissions mechanism.

However, I've not worked out for myself just how far I should go beyond this. Some of these students will be system administrators or systems programmers. Others will be managers responsible for policies regarding computer installation and "security." Some others, however, may be irresponsible types, looking for a laugh or a way to screw their fellow human. So, do I teach them about the historical security holes in Unix systems? Do I tell them that if they have privileges on their workstation, many of these privileges can be applied on the fileserver if they have an account there? Do I explain how the famous RTM Internet Worm exploited bugs? Do I cover how one can capture keystrokes in the X-windows environment?

In short, do I do more harm than good or vice versa? I've heard most of the standard arguments and tend to feel that what is known should be passed on, but I'm interested to hear your views.

fc <FBCohen@dockmaster.ncsc.mil>:

First, I think that your point should be placed on Risks so that all of

the others on that list can understand your concerns. More importantly, this issue is fundamental to many peoples' view of protection issues.

I will briefly explain my feelings on this matterhere, but for a much more thorough coverage, you should probably give me a call - [I've deleted his number; he didn't specifically say that I might post it.]

The basic issue is what we should teach about protection to students in light of the fact some might use if for evil. I think that there is a lot of information on how to attack systems available to anyone who wants it, but there is too little information on defenses for those who wish to protect themselves. In light of this imbalance, it is clear what to do, if you believe it.

When I teach people about protection, I don't necessarily discuss all of the attacks in order to point out defenses. A fundamental thing that most people don't understand is that protection is not an excersize in attack and defense, but rather an excersize in design for integrity, privacy, availabilit, and accountability. You could present it in this positive light without talking about attacks at all. In fault tolerant computing we discuss failures, often leaving out the mechanism by which the fault occurs. We still want continued operation, and can describe it in terms of proobabilities of events regardless of causes.

In terms of teaching about how to break into systems, I think it is important to every user to understand how people guess passwords, if only to help them understand how to choose their own passwords. I think that they should understand the concept of a Trojan horse, and that when they run another user's program, they can have all of their protection bits changed (etc.). If you don't know this, you might (and most do) assume that setting a protection bit in Unix makes you safe. So we teach people a lot of assumptions about protection (if only by telling them that setting a bit prevents something from happenning), and these assumptions are almost always wrong, and as a result, they are vulnerable. Perhaps you could simply be very careful about the assumptions you leave your students with. (e.g. ANY program can set the protection bits of any files owned by the user running it - for example, the "chmod program" provides a handy user interface to this, while other programs set protection bits without the user getting involved.) Some bright student will likely ask whether this means that their protection bits can be set whenever they run another user's program, and you should answer "yes!" (note the emphasis). Take that chance to also point out that this is why you don't run their programs from your account - after all, we wouldn't want their grades accidentally protected so that other could read (or modify) them. (you do take this precaution - yes?).

Having taught protection for many years in universities, I have faced these moral issues on many occasions. I can say that the delicacy of modern systems is a surprise to my students, and they walk away a bit more careful than when they entered, which I think is a good thing.

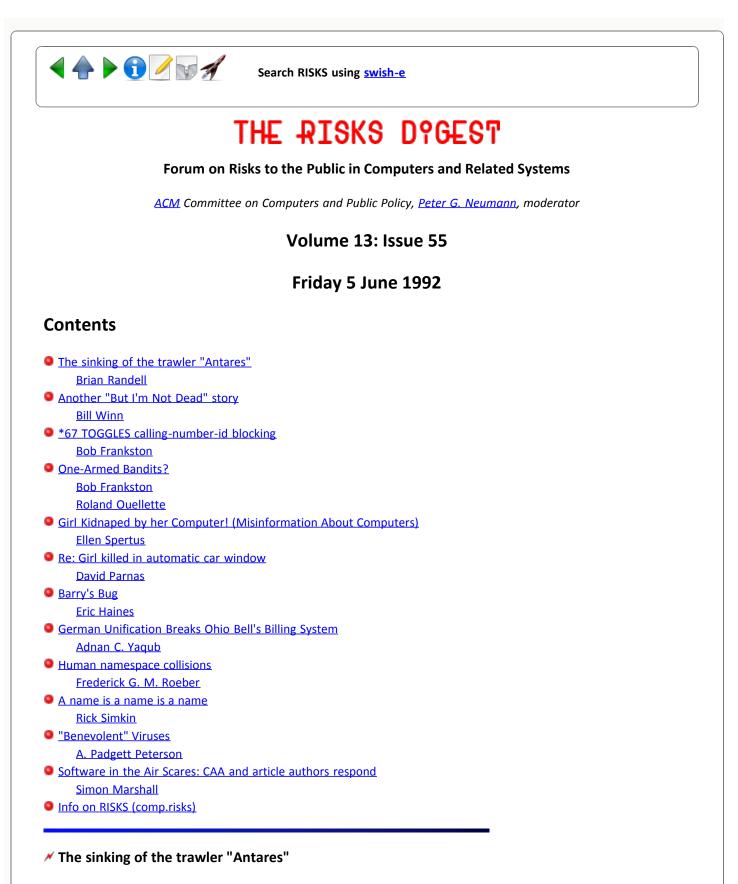
When you teach about operating systems, do you point out that the internal OS tables are generally not allocated the "worst case" amount of space they may require? You know that in practice, designing systems in this way is commonplace because the total resources is not sufficient to handle worst case, but we don't want to artificialy limit things. This is a common cause of protection problems - leaving temporary files around because of the process failures that result, overrunning available memory and overwriting some OS code, not being able to handle a critical interrupt, etc. Most of the programmers I know don't check every possible return code on each OS call and act appropriately by undoing everything they should when the failure takes place, and no current language I am aware of provides the means to handle these issues appropriately. None of these things require that you discuss attacks, but rather are simple realities your students should understand when writing their code, along with the knowledge that most programmers don't properly deal with these things.

Well, my list goes on for books worth - perhaps you should get some of them for your own interest. Call me for details. FC



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<Brian.Randell@newcastle.ac.uk> Fri, 5 Jun 1992 09:44:56 +0100

[Here is an article about an on-going court martial in the UK. The sort of situation and allegations discussed are well-known to RISKs readers, so I

have provided the quote essentially just for the record. Brian Randell Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 ]

COMPUTER BLAMED FOR SEA COLLISION (The Independent, 5 Jun 1992)

A Trainee submarine commander yesterday blamed a computer error for an accident which sank a trawler and killed four Scottish fishermen. Lieutenant Commander Peter McDonnell told a court martial at HMS Drake in Plymouth that he trusted HMS Trenchant's computer system when it told him he was at least three miles away from a possible collision with the Scottish trawler Antares. He said his generation of submariners preferred to rely on the computer rather than a manual plotting system which a senior submarine captain earlier told the hearing was a more trustworthy method in busy waters.

Four men died in November 1990 when the Antares was dragged to the bottom of the Firth of Clyde by HMS Trenchant. Lt Cdr McDonnell, 33, from Glossop, Derbyshire, had just completed the last exercise of a six-month command course known as the Perisher when the accident occurred at 2.18am. He denies six charges of negligence. Yesterday he told the hearing that he had not even known that Trenchant had passed close to the Antares and another fishing boat five minutes before he ordered the submarine to turn around and head back towards them.

The hearing continues today.

[Ross.Anderson@cl.cam.ac.uk found most of that in The London Times as well.]

# Another "But I'm Not Dead" story

<tcemail!pc!Bill\_Winn@uunet.UU.NET> Wed, 3 JUN 92 15:27:41 EST

SORRY, BUDDY - IT SAYS RIGHT HERE THAT YOU'RE DEAD (Indianapolis Star, June 3, 1992)

And you think you've had trouble dealing with apathetic bureaucrats?

Meet Eugene Smith of Doylestown, PA. The healthy 33-year-old has spent the past 2.5 years convincing authorities he's not dead. The frustrating error cost him his driver's license and his job. He still can't get a license, and he's still fighting nine traffic violations that he says aren't his. Smith traces the trouble to the theft of his wallet in 1988. He believes the thief used his driver's license, racked up violations that led to the license suspension, then died in a traffic accident.

In February 1990, a police officer stopped Smith and told him his car registration was expired and that state computer records showed he was dead. "He said I was dead, and because of that I was not allowed to drive," said Smith. "I agreed that it would be [a] hazard for a dead person to be driving." Life isn't easy for an officially dead man. Without a license, Smith lost his job as a driver for a warehouse. Without that job, he had to find a cheaper place to live and take a job nearby, at a deli. Being an officially dead taxpayer, no one in the state capital took him seriously. "I would call and I could hear them say, `Oh, this is that guy again,' and I could hear them laugh and they would say nobody there could help me," Smith said.

Finally, Susan Rakus, an aide to Democratic U.S. Rep. Peter Kostmayer, took his case and persuaded the state motor vehicle agency to resurrect Smith [isn't this against separation of church and state?]. But Smith still can't get a license -- he's still accused of a string of years-old traffic violations.

"Obviously we dropped the ball on this," Rick Schoen, state transportation department spokesman, said Tuesday.

William Joseph Winn bill\_winn@pc.indy.tce.com

## \*67 TOGGLES caller-id blocking

<Bob\_Frankston@frankston.com> Thu 4 Jun 1992 00:13 -0400

There has been a discussion going on in the Telecom forum about \*67 which TOGGLES(!!!!!) the caller-id blocking state of a phone line -- at least in those areas with caller-id blocking. The rationale for requiring caller-id blocking in some states is that there are situations where disclosing one's location might be life-threatening as in the case of a shelter for battered women or maybe a protected witness. Of course, there are also normal privacy considerations.

If one always was sure of the default state of the line one was using a toggle might work. But there is no way to determine the state beyond faith that the telco's computer is exactly synchronized with one's expectations and that one has is using the assumed CO lines on multi-line systems. If one is a visitor, all bets are off. As from plain errors made in the business office or at the CO, one reader pointed out that one some switches reloading the software loses the settings. Another reader pointed out that \*67 isn't an accident but the specified behavior.

The stupidity (the word risk doesn't do justice to the situation) is obvious. I'm more puzzled about how it came about. I generally lean towards incompetence as an explanation rather than conspiracy but since some of the rationale for requiring caller-id comes from public safety considerations, I'm surprised that no one has challenged this approach as failing to satisfy this requirement and, by providing the illusion of caller-id blocking, might increase the risk.

While on this subject, there is also the issue of access control over information passed via signalling protocols. Telcos are assumed to have full access and subscribers none. But some organizations can act as their own telcos. The MIT ISDN switch comes to mind. Which side of the protection barrier are they on? ANI is similar to caller-id but is nonblocked and delivered when calling an 800 #. This means that if I give out my personal 800#, I will eventually (on the next bill) get their #.

### ✓ One-Armed Bandits?

<Bob\_Frankston@frankston.com> Thu 4 Jun 1992 09:31 -0400

In today's Wall Street Journal, there was a feature piece on a slot machine tournament in Atlantic City. The problem was that the machines were returning a 70.6% payoff rather than the 96.4% planned. "After the tournament ended and the prizes were awarded, the manufacturer called back to report that the two kinds of chips it shipped were incompatible with each other". Aside from all the issues of how this might have happened, the real danger is soft failure that are hard to detect. The only reason someone even looked for a problem was the unique circumstances of a tournament which provided an environment to notice the statistical anomalies Apparently there is no constant checking to see that the statistical results match the predicted results.

The \*67 (above) and this story both illustrate a risk of not understanding the philosophical (as well as engineering) concept of closed-loop systems, i.e., those with feedback so that one can determine the result of an action. This is a lesson that should feedback to nontechnology systems also.

[Chuck Weinstock <weinstoc@SEI.CMU.EDU> also noted the slot machine saga, as did Roland Ouellette, who added the note that follows. PGN

## ✓ One-armed bandits too efficient

Roland Ouellette <ouellette@tarkin.enet.dec.com> Fri, 5 Jun 92 09:59:08 EDT

This makes me wonder if anyone actually tests these machines: people at the factory or regulators at the casinos. Also would this sort of error be noticed only with an event like this and ordinarily go undetected?

**Roland Ouellette** 

# *H* Girl Kidnaped by her Computer! (Misinformation About Computers)

Ellen Spertus <ellens@ai.mit.edu> Thu, 4 Jun 92 15:21:46 EDT

I've had up on my door an article from the 4/14/92 Weekly World News an American tabloid) with a headline: "Girl, 13, kidnaped by her computer!" Here is an excerpt:

A desperate plea for help on a computer screen and a girl vanishing into thin air has everyone baffled ---

and a high-tech computer game is the prime suspect.

Game creator and computer expert Christian Lambert believes a glitch in his game Mindbender might have caused a computer to swallow 13-year-old Patrice Toussaint into her computer.

"Mindbender is only supposed to have eight levels," Lambert said. "But this one version somehow has an extra level. A level that is not supposed to be there! The only thing I can figure out now is that she's playing the ninth level --- inside the machine!"....

Lambert speculates that if she is in the computer, the only way out for her is if she wins the game. But it's difficult to know for sure how long it will take, Lambert said.

"As long as her parents don't turn off the machine Patrice will be safe," he said. "The rest is up to her."

Why am I posting this to comp.risks? Do I really think there is a risk of people being kidnaped by computers? No (although at times, when I work on my thesis, I wonder.) The risk is the misinformation people receive about computers. I don't worry too much about the WWN, but I was concerned about an educational show I watched last night, Mathnet, based on a segment of the PBS educational television show, Square One. Mathnet is a spoof of the detective show Dragnet, and the detectives use math to solve crimes. So far, so good, but on last night's episode, the crime they solved was the kidnaping of a baseball player whose disappearance had been unnoticed because he had been replaced by an android which had been able to talk and play baseball. An educational show would not show space aliens or magic, so the implication of including human-like robots is that they are technically feasible.

Similarly, when I recently visited Epcot, an amusement park that is supposed to be educational, the computer exhibit featured an electronic character that was able to understand and even physically transport its human companion.

I expect (and enjoy) such unrealism in tabloids and in science fiction, but it should not appear in educational settings. I suspect that a large percentage of people, if asked, would say that a robot could currently be built that could pass as human, based on all the misinformation they receive. Ellen Spertus

## Ke: Girl killed in automatic car window (Ian Spalding)

David Parnas <parnas@qusunt.eng.McMaster.CA> Wed, 3 Jun 1992 16:46:21 -0400

Isn't it just like our technocratic society to react to such an accident, caused by a completely unnecessary luxury becoming too complex, by making it even more complex? Wouldn't the simpler solution be to ban automatic windows or even power windows instead of requiring another safety interlock? Nobody needs such things but, unfortunately, there are car models in which you can't get an ABS (good thing) without buying power windows (artificially induced desire). I told my dealer that I was willing to pay extra for manual windows, but could not get them.

## 🗡 Barry's Bug

Eric Haines <erich@eye.com> Thu, 4 Jun 92 09:34:57 -0400

Viruses are a dime a dozen nowadays, but I thought this one was of particular interest (though I do have to wonder if the issue of "Computing" magazine was from April 1st...).

>From Communications of the ACM, June 1992 (vol.35, no.6), page 10:

Barry's Bug...

Viruses, as we all know, can play strange and frightening games with computer-based data. Now, "Computing" magazine has reported a new strain that plays some strange, and yes, frightening music. It's called the Barry Manilow Virus - a phantom bug that's infiltrating a growing number of computer systems, scaring users with such tunes as "Mandy" and "Copacabana." The virus is a collection from the singer's "Greatest Hits" album. Once detonated, the virus spins out a continuous stream of Manilow's million sellers. Experts are working feverishly on an antidote for this plague. -- Eric Haines

## ✓ German Unification Breaks Ohio Bell's Billing System

Adnan C. Yaqub <adnan@odin.icd.ab.com> Fri, 5 Jun 1992 21:44:51 GMT

My family is enrolled in AT&T's World Reach-out plan. This plan provides discounted calls to many countries throughout the world during designated times, including what used to be West Germany. However there are no discounts to what used to be East Germany (GDR). At our house, we call Germany (the western part) a lot.

Yesterday we received our May phone bill from Ohio Bell. I noticed that after around May 5 our calls to Germany did not have the Reach-out discount. Also, the designation of the location called was changed from "Ger Fed Rep" to "Germany".

I called AT&T, and a rate adjuster told me that the problem was with Ohio Bell's billing software. It seems that their software was keying off the "Ger Fed Rep" to apply the Reach-out discount, not the country code (49). Thus, in May, when AT&T decided to change the designation "Ger Fed Rep" to "Germany", the software broke. AT&T credited me the difference, which was \$21.00. I wonder how many other phone companies will have the same problem and how many other people will be affected.

Adnan Yaqub (adnan@icd.ab.com) Allen-Bradley Company, Inc., 747 Alpha Drive, Highland Hts., OH 44143, USA Phone: +1 216 646 4670 FAX: +1 216 646 4484

## Human namespace collisions (Re: Earnest, <u>RISKS-13.54</u>)

<roeber@vxcrna.cern.ch> Fri, 5 Jun 1992 21:46:29 GMT

With the increasing amount of casual communication these computer networks (like usenet) are encouraging, this namespace collision situation is likely to increase. I recently experienced this.

A few months ago, I posted an article to comp.realtime which quoted the US GAO report on the Patriot missile failure. Somebody read it there, and reposted it to the widely-read comp.risks forum. Shortly thereafter, I received an e-mail message from another person named Fred Roeber. He works for Raytheon, the makers of the Patriot system! His father, also named Fred Roeber, also works for Raytheon. He saw my article, and immediately fired off letters to his superiors, alerting them that the posting was \*not\* inside information from either one of them, but public information from someone with the same name.

Luckily, it seems that no harm has come from this. In fact, two branches of a family that hadn't known about each other can now fill in some gaps in the family tree. But if one of his superiors had seen the article first, and acted prematurely; or if the GAO or I had made a mistake that Raytheon might have considered slanderous, the results could have been much worse for him.

The RISK seems to me to be that if we do not realize just how large this increasingly popular global community is, we may mis-estimate the probability of such a collision, and make mistaken assumptions about identity.

Frederick G. M. Roeber | CERN -- European Center for Nuclear Research e-mail: roeber@cern.ch or roeber@caltech.edu | work: +41 22 767 31 80 r-mail: CERN/PPE, 1211 Geneva 23, Switzerland | home: +33 50 42 19 44

### A name is a name is a name

Rick Simkin <rsimkin@dlogics.dlogics.com> Fri, 5 Jun 92 10:05:06 CDT

A little over a year ago, I was hounded by a collection agency for debts owed by Richard Simkin, a car dealer in northern Illinois. It took about a month (and a letter to the Better Business Bureau) to convince the agency that I wasn't their man.

Late last fall, I applied for and received a Discover Card. About 4 months later, Discover Merchant Services decided that my name matched that of Richard

Simkin of Roselle Motors and tried to collect his debts from me.

The pattern was to leave a phone message, or send a letter, telling me to call Ranee. Phone messages (especially the first time, when all this was news to me) never said why I should call. When I would call, Ranee was never in the office, so I'd end up talking to someone else. I'd explain that I wasn't a car dealer, and that they'd mixed me up with somebody else. They'd promise to take care of the problem; once a supervisor told me that I shouldn't have gotten a letter at all--he couldn't even figure out how it got to me, since my address wasn't on the record of the delinquent merchant--and I should ignore it.

I've cancelled my account now, hoping that if there's no customer record, they won't match it to their merchant record. I'm told that Discover policy requires more than a matching name to claim that two records represent the same person; and that by that policy, my record does not match that of the car dealer's.

Computer Risks:

- Computer programs don't always reflect company policy.
- Flexible tools (such as a database query language and mail merge) provide an easy means to act on wrong assumptions, and don't always leave audit trails the way tailored applications can.

Rick Simkin	UUCP:	uunet!	dlogics!rsimkin
Datalogics, Inc.	INTERNET: rsimkin@dlogics.com		
441 W. Huron St.	PHON	NE: +1	312 2664437
Chicago, Illinois 60610-3498	USA	FAX:	+1 312 2664473

# "Benevolent" Viruses (Ts'o, <u>RISKS-13.54</u>)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Thu, 4 Jun 92 08:24:59 -0400

>It all boils down to what your definition of "virus". My definition of "virus"
>is a piece of software which transmits itself from machine to machine without
>the knowledge or permission of either a user on the system or the system
>administrator of the machine.

While I agree with the first part, I must disagree with the second. A virus is nothing more than a propagating program. "Knowledge or permission" has nothing to do with the purpose of a virus. The only factor that is necessary is some sort of rules base to maximise the probability of viable propagation.

Personally, I deplore the common use of viruses primarily because it is inherently destructive whether or not the programmer was intentionally malicious. The current crop of PC viruses (what most people know as viruses is a function of personal computers - single tasking unprotected architectures) is obviously only a subset of Dr. Cohen's envelope.

The incredible diversity of what the world considers a "PC" is what makes even the most innocuous virus destructive in some cases. Take STONED for example. It has only two functions: 1) To propagate 2) To occasionally display a message. The fact that it (and its close variants) are statistically the most common virus in the world today indicates that it is very good at (1).

However, in some cases, probably not understood by its creator, STONED is destructive. Hard disks created without any hidden sectors (early FDISK), floppy disks with nearly full root directories, and UNIX systems may become unusable.

This type of problem also occurs with professional software and any reader can name major products that would not run on a particular machine. (Years ago the true test of a "100% compatible" PC was whether or not it could run "Flight Simulator" properly. The interesting thing about FS was that the early versions ran without any operating system, you just booted the PC with the FS disk in "A:").

The point that I am trying to make is that very few people really understand PC architectures at the BIOS/Microcode level and this is necessary to be able to write "safe" low-level code. Most viruses are not intentionally destructive, however their mistakes often have the same effect. Consequently, while I can conceive of a "benevolent" virus, I would not necessarily trust one on my systems.

Having said that, consider the following case: a LAN server that as part of the logon script checks the client for the presence of resident security software, verifies its integrity, and automatically updates the software on the client if missing or an older version. This would meet the test of software that is self-propagating and rules based. Even if user intervention is required to continue, given the alternative of being denied access to the LAN, few will refuse. Is this a "benevolent" virus ? (can give commercial examples). Padgett

## Software in the Air Scares: CAA and article authors respond

<Simon Marshall <S.Marshall@sequent.cc.hull.ac.uk>S> Thu, 4 Jun 1992 22:01:09 +0000

In <u>RISKS-13.50</u>, I reported an article concerning software errors in auto-pilots of Boeings flown by British Airways, which appeared on the front page of the ``Sunday Telegraph'', May 17. My reason was to bring attention to the article's content, which was that there were ``10 serious incidents involving computer errors in January'' with BA.

I then made a number of comments, principally that this appeared to be a high incidence rate; that the errors occurred in auto-pilots which I assumed to be relatively simple systems (as compared to fly-by-wire) in which there is much experience of design; that a comment made by a British Airways spokesman that the software was CAA approved and tested for 100 hours before entering service hardly reassuring.

Imagine my surprise when I received a phone call a week later from an exasperated Dan Hawkes of the CAA. I am reporting this more than a week after the fact, largely from memory. His main complaint was that the article had

been quoted without question, and that so often (as we know from newspaper reporting of our own fields) these articles are of dubious reliability and sensational. He made a further comment that he felt that academic input to the issue of software reliability in aircraft was largely negative.

He reported to me that the software problems in the auto-pilots arose as a result of a modification to software; the cause had been rapidly located and fixed. Recovering from the initial shock of his call, I attempted to don a journalistic hat and ask a number of questions.

I suggested that the MTBF of 10<sup>-9</sup> for software is unverifiable. This he was happy to agree with, but stated that auditing and monitoring of all stages of the software design and development gave a high level of confidence in its performance. Overall design meant that no single possible on-board failure (be it software of mechanical) could result in loss of aircraft integrity. He stated that as all of these involved auto-pilots, there was never any danger to the aircraft as pilots are always there to take remedial action when necessary. In effect, that these were not serious errors at all. I think Nancy Leveson (a name he was familiar with - ``an academic'') has pointed out the dangers of making highly trained pilots into computer monitors.

I then raised the point that this certainly cannot apply to fly-by-wire software, as in this situation pilots are not monitors but dependent users. His answer was that the auditing and monitoring is more rigorous in the design and development of fly-by-wire, and that (to paraphrase) ``there have not been any failures yet". Again his message was re-assurance; there is no serious risk. I could not get a real answer as to where the 10^-9 figure came from.

I then decided to attempt to get in contact with the authors of the original article, Robert Matthews and Christopher Elliot. Robert Matthews (Science Correspondent) told me that the basis of the article had come from Flywise (as pointed out by Martyn Thomas, <u>RISKS-13.51</u>), and had been checked out with BALPA (union), BA and CAA (who were ``not all that helpful'') before publication. He stood by the article, and added that the airline companies and authorities were a closed world, and getting any information from them near impossible. Sounds familiar? He had not received any satisfactory explanation of the software reliability figure of 10^-9.

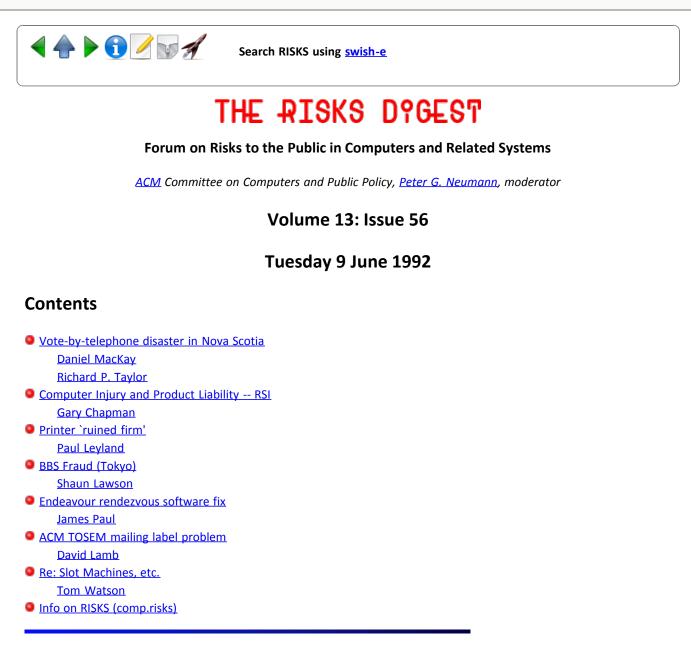
I swapped sources; a few issues of RISKS for a few tidbits from him. The issue of Flywise states that the software incidents were due to ``software design defect[s]". An interesting titbit was a paper from Boeing on structural airworthiness. According to their figures, in terms of hull loss rates per departures, to 1988 the A320 was worse than any other commercial jet since the Comet. Though none due to software; that hasn't happened yet.

Simon Marshall, Dept. of Computer Science, University of Hull, Hull HU6 7RX, UK Email: S.Marshall@Hull.ac.uk Phone: +44 482 465181 Fax: 466666



Search RISKS using swish-e

Report problems with the web pages to the maintainer



### Vote-by-telephone disaster in Nova Scotia

Daniel MacKay <daniel@nstn.ns.ca> Sun, 7 Jun 92 13:38:09 ADT

Well, I'm pretty close to the source, so I thought I'd write about it.

Some time ago, the Liberal party of the province decided they'd use a high-tech voting system, fairly simple in structure. They would contract with the local telco, Martime Tel and Tel, to use a phone/computerized phone system so that people could vote from the main leadership convention here in Halifax or from regional rallies (where they had banks of phones installed) or from home using their touchtone phones.

The method:

- 1) Each candidate got a 1-900- number.
- 2) Each card-carrying Liberal would get a PIN and instructions.

- 3) Come convention day, each Liberal could dial the number for the candidate of his or her choice, the candidate's recorded voice would state for whom that vote was about to be cast, and request the Liberal to enter the PIN.
- 4) After entering it, the candidate would thank the Liberal for his or her vote, and hang up.

Voting was supposed to begin at 12:30, and take 90 minutes for the first round. If necessary, several voting rounds could be cast during the day.

Everything went wrong.

A chronology:

- 12:30 Voting begins. However, voters do not get the thank you after entering their PIN.
- 12:35 Confusion takes the throne, and reigns for the rest of the day. Some telco reps said that your vote was registered even if you didn't get a thank-you. Others said that the votes were being counted, don't worry.
- ~1:00 Voting is suspended while everyone works things out.
- 1:40 The electoral officer announces that all votes will be cancelled, and that voting will begin again at 2:30.
- 2:00 A kid with a scanner calls the Canadian Broadcasting Corporation to tell them that he has a recording of the Party's conversation with the telco via celphone, giving the results so far. The CBC passes the report up their hierarchy, trying to decide if it's a faked report. The kid calls back thirty seconds later with the contents of \*their\* conversation with an Executive Producer, also by celphone. The CBC decides to run the story.
- 2:30 Voting begins again. Callers are instructed that unless they get the thank-you message, their vote has not been counted. Some people get a thank-you on the first try, others try for 20 or 30 times. In a desperate move, the telco cuts down on the number of circuits into the system, to no avail. Voters now have busy signals as well as no acknowledgements to deal with; they report that the far end phone either sends the thank-you within a few seconds, or does nothing for about ten minutes before hanging up.
- 3:00 Voting is extended until 4:00. Many voters complain that their PIN is being rejected. Officials say to never mind, just try to vote again in this case.
- 4:00 Less than half the conventioneers have voted. Voting is extended until 5:00.
- 5:00 Voting is extended until 6:30.
- 5:30 Reports begin arriving that members have been able to vote twice.
- 6:30 The convention is called off.

What went wrong? System-design-wise? Considering the PIN as a password -each member knew only his -- there was no UID (member number) to PIN matching. So anyone who knew your PIN could vote on your behalf. So the problems of a) PINs being rejected, and b) voting twice could easily be explained as people making finger errors. If you made a mistake with your PIN, either you got someone else's number and voted for them, or you got rejected -- no way to tell. If you later went back and used your correct PIN after having used someone else's, why, that would look a lot like being able to vote twice. Users couldn't, of course, change their PINs. Anyone with a programmable dialler could have voted for many, many Liberals if he knew the format of the PINs. Given the profoundly bad management we saw, I wouldn't be surprised to see them as six-digit numbers ranging from 100001 to 107290; there were 7289 registered voters. This prospect hasn't even been discussed yet in the local media.

There was no backup voting system for this, the inaugural use of the system. The telco convinced the Party there was no need for it -- the telco (the newspaper report says) reminded the Party that it handles hundreds of thousands a call a day, and there was no possibility of the system failing.

Operationally, there was either a bug in the voting software, or it was incapable of handling the volume of traffic, causing it to fail to thank-you most of the time. And, of course, the kid with the scanner telling all just added icing to the cake.

It was not a great day for the telco, or for the Liberal Party. There hasn't been any discussion of responsibility, but there sure will be next week! The convention cost hundreds of thousands of dollars, and it was \*entirely\* a wasted effort.

Daniel MacKay, NOC Manager, NSTN Operations Centre, Dalhousie University, Halifax, Nova Scotia, Canada daniel@nstn.ns.ca 902-494-NSTN

[The METHODS paragraph above was lightly edited by PGN for clarity.] [This case was also reported by Richard Taylor of AECB, Aidan Evans <AE@AC.DAL.CA>, and parnas@triose.eng.McMaster.CA (Dave Parnas).] [Another example of a case for public key encryption? PGN]

### Phone-in Voting in Nova Scotia

<atomcon/I=R/S=TAYLOR/O=AECB.CCEA@mhs.attmail.com> Mon Jun 8 13:46:17 -0800 1992

[WARNING: ATTMAIL may reject this address. It has been doing so for weeks for all RISKS mailings. Richard included extracts from a Canadian Press article by Alan Jeffers in The Ottawa Citizen, Sunday, June 7, 1992, not included here, along with the following comment:]

Again on CBC Radio this morning: there is now talk about having to run the entire campaign over again since the candidates who were listed as faring badly in the cellular telephone message are protesting that this disadvantages them in a new polling. A second campaign would severely drain the resources of the party and would put them at a disadvatage in subsequent elections. RPT

Richard P. Taylor, Ottawa, Canada.

#### Computer Injury and Product Liability

Gary Chapman <chapman@silver.lcs.mit.edu> Mon, 8 Jun 92 10:14:22 -0400

The lead story in the business section of the New York Times 8 Jun 1992 says that "a surge of litigation" is expected in cases alleging repetitive strain injury (RSI) caused by information-based equipment, "pitting telephone operators, supermarket cashiers, journalists, and a wide variety of clerical workers against many of the world's biggest manufacturers and a number of smaller makers of high technology equipment."

The reason for this "surge," says the article, is last week's ruling by a Federal Court in Brooklyn consolidating plaintiff cases of all hand, arm, and wrist injuries allegedly caused by using high tech equipment, especially keyboards. There are 57 defendants in the case that the Court ruled on last week, including IBM, AT&T, Unisys, DEC, Apple, Xerox, Eastman Kodak, and Hewlett Packard. The defendants also include the U.S. subsidiaries of Northern Telecom, Sony, NEC, Fujitsu, Samsung, and Phillips.

The article says that victims of RSI have previously relied on workers' compensation awards, but workers' compensation does not provide for judgments based on pain and suffering or on negligence on the part of the defendants. The Federal Court's ruling last week will allow plaintiffs to sue manufacturers under product liability laws, which means jury trials and, potentially, punitive damages, although the latter seems unlikely.

RSI injuries are potentially one of the largest pools of product liability cases in the country. The article says that the Bureau of Labor Statistics estimates that 45 million people use computers on the job in the United States.

Consolidation of cases has risks to both sides of a product liability dispute. Rulings and decisions in a consolidated case can affect thousands of plaintiffs, so if the case comes before a judge with a tendency to rule in favor of one side or the other, the effects of the rulings are magnified. The judge in the subject case consolidated the plaintiffs' cases in order to get a baseline of scientific testimony on the connection between computer equipment and RSI, but that could mean that companies that have taken more care in terms of equipment safety could be lumped with companies that haven't done anything. Plaintiffs have the advantages of seeing their case come to trial sooner and getting better testimony from top expert witnesses, as well as sharing the risk of failure, but they tend to get lower awards when they share a judgment or a settlement than if their case was successfully tried on its own.

The judge in Brooklyn, Judge Jack B. Weinstein, said that the decision to consolidate does not rule out the possibility that the cases may be separated in the future, or that they could be dismissed altogether. Judge Weinstein is one of the most famous figures in American product liability law, having presided over the consolidation of cases involving asbestos (the world's largest product liability pool to date), Agent Orange, and DES (diethylstilbestrol).

Gary Chapman, Coordinator, The 21st Century Project chapman@lcs.mit.edu Computer Professionals for Social Responsibility, Cambridge, Massachusetts

# "Printer `ruined firm'"

Paul Leyland <pcl@ox.ac.uk> Tue, 9 Jun 92 13:23:06 +0100

A printer who thought that his employers were trying to avoid paying him \pounds 2,000 he believed was owed hacked [sic] into the firm's computer and disabled the machine, Southwark Crown Court, south London was told yesterday. Richard Goulden, 35, a freelance typesetter of Uxbridge, west London, who had used a password that only he knew, refused to free the computer until the firm, Ampersand Typesetting Ltd, of Camden, north London, had paid up. The computer refused and, after allegedly losing more than \pounds 36,000 of business because it did not have access to information on the computer, went bankrupt. The prosecution claims that Mr Goulden's action contributed to the bankruptcy. Mr Goulden denies illegal modification of computer material under the 1990 Computer Misuse Act. [\_The Times\_, London, 9 June 1992]

# BBS Fraud (Tokyo)

Shaun Lawson <shaun@isr.recruit.co.jp> Mon, 8 Jun 92 10:06:27 JST

This is a summarized translation from Japanese of a posting of H. Murakami (mhiroshi@tansei.cc.u-tokyo.ac.jp) regarding the use of a bulletin board service in Japan to commit fraud.

Method:

- 1) The perpetrator opens a BBS.
- 2) Passwords and E-mail addresses are collected.
- The passwords and E-mail addresses are used to gain access to the BBS users Nifty Serve or PC-VAN accounts. (Similar to Compuserve and Prodigy)
- 4) The passwords of these accounts are changed to prevent access of the real users.
- 5) A bank account is opened under an assumed name.
- 6) 'For Sale' notices for PC's etc. at low prices are posted from the stolen accounts.
- 7) Victims replying to the postings are requested to transfer money into the bogus bank account.
- 8) The money is withdrawn and the victims are out of luck.

The police were able to arrest the perpetrator after his face was recorded by bank security cameras when he withdrew the money.

Morals of this story:

- A) Use different passwords for different accounts.
- B) Log on regularly to check for irregularities.

Shaun Lawson, Institute for Supercomputing Research, 1-13-1 Kachidoki, Chuo-ku,Tokyo, Japan 104(03)3536-7770shaun@isr.recruit.co.jp

### ✓ Endeavour rendezvous software fix

James Paul <jpaul@nsf.gov> Mon, 08 Jun 92 15:53:25 EDT

Aviation Week and Space Technology (8 June '92, p. 69) states that "NASA Will Modify Rendezvous Software To Avoid Repeat of Endeavour Problem" The article reads:

NASA will change the specifications on the IBM software used to calculate space shuttle rendezvous maneuvers to avoid problems on future missions like the one that occurred at a critical point during Endeavour's final rendezvous with the Hughes/ Intelsat 6/F3 spacecraft (AW&ST May 25, p. 79).

Engineers have traced the problem to the sensitivity of NASA-developed equations to a particular set of numeric values that arose when Endeavour was making one of the final computer-targeted rendezvous maneuvers. Test show the software had been properly coded by IBM and therefore passed all preflight tests, according to Ted Keller, senior technical staff member at the IBM Shuttle Project Coordination Office, Houston.

The numerical values that caused the problem so closely resembled each other that the software recognized them as identical values -- which they were not. This resulted in the software providing incorrect targeting data for the maneuver.

By relaxing the tolerances in the software, orbiter computers should be better able to differentiate between values that are similar and provide proper targeting information, Keller said.

# ACM TOSEM mailing label problem

# David Lamb <dalamb@qucis.queensu.ca> Mon, 8 Jun 1992 13:53:52 GMT

This might be "the risks of asking for subscriptions 2 years before you can deliver any issues": I received 3 copies of the 2nd issue of ACM TOSEM (Software Engineering and Methodology) last week. I called up ACM Member Services and they said there had been "a problem printing the mailing labels" (which, at least, they didn't blame on "the computer". A careful examinination of the labels shows they're all identical, except one says "EXP 9012", another "EXP 9112", and the third "EXP 9212". It's nearly certain those are a series of dates on which my ACM membership expires (it's a common practice with subscriptions these days to include the expiry date on the mailing label).

I got to thinking after the phone call about how this problem might have occurred. I'm quite absent-minded, as befits an academic, but I think I signed up for TOSEM as soon as ACM announced it, which may well have been back in 1990. At some point, perhaps later in 1990 when I paid my dues, I paid for a subscription. The first issue came out in January 1992; I wonder if some attempt to remember ACM's multi-year obligation to send things to me resulted in records for each of the 3 years? It doesn't explain why the problem didn't occur with the first issue.

If a lot of people had such a problem, it may well have cost ACM a lot of money.

# Ke: Slot Machines, etc. (Frankston, Ouellette, <u>RISKS-13.55</u>)

Tom Watson <johana!tsw@apple.com> Mon, 8 Jun 92 20:16:09 -0700

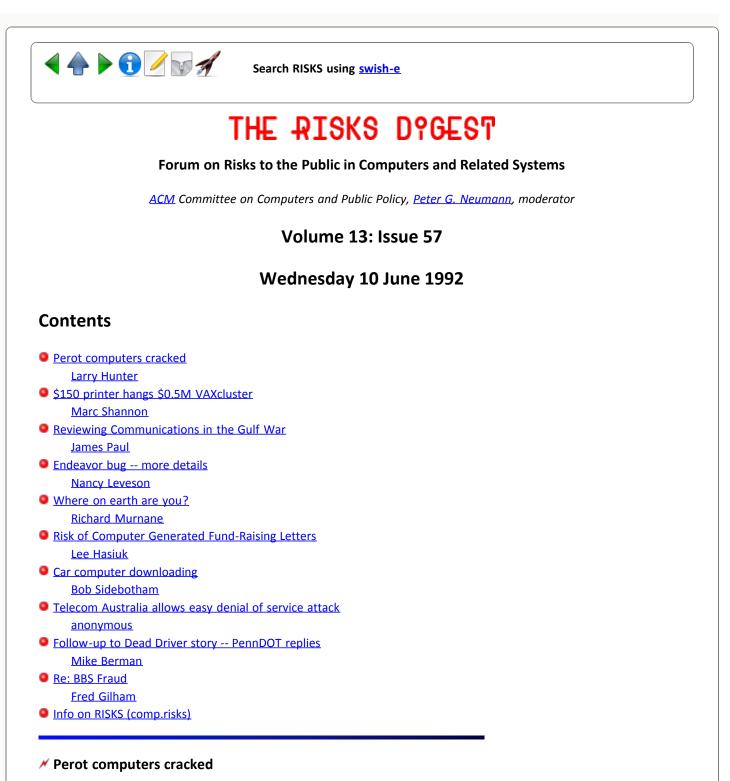
I read several years ago (Datamation, or some similar 'free' magazine) that there is an offical testing lab in New Jersey (for Atlantic City) that tests these things. In order to be 'certified' they need to produce the software in source form, the diagrams of the circiuts, and copies of the ROM's used in the machines. The testing lab used all sorts of tools (ICE's Logic Analyzers, etc.) to verify that the opeation of the game (Slot Machine, Video Poker, etc.) was up to specification (odds, etc.). The article went on to say that the testing lab did all it could to prevent non-random payoffs (not too cool). It sounds as though the testing was not complete for the given games, or the testing facility (funded part of gaming commission) was not funded. Perhaps someone else can remember the exact article, as it has been a few years (probably about 4 or so) since I saw it.

Tom Watson, johana!tsw@apple.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Larry Hunter <hunter@work.nlm.nih.gov>

10 Jun 92 11:32:10

Richmond, June 9 (AP) -- An intruder erased information on about 17,000 supporters of Ross Perot from a computer file at the undeclared Presidential Candidate's Virgina headquarters, campaign officials said. They added, however, that they have copies of the files destroyed in the weekend incident.

The data included the names, addresses, telephone numbers and notes on about 17,000 Perot supporters in Virginia. "It's not a political act as far as I'm

concerned," said Mark Adams, the state petition coordinator for Virginians for Perot. "I don't feel threatened by anything of that nature." [From the NY Times, 10Jun 1992, p. A20]

I understand that the spokesperson for the campaign would want to downplay the importance of the incident, and say that he didn't feel threatened, but it is hard to avoid the conclusion that this is a politically motivated dirty trick. The Virginia election petition filing deadline is less than 3 weeks away.

With a hotly contested and unusually complicated Presidential election upon us, I would hope that electoral computer risks will be receiving heightened attention from the community of computer professionals.

Lawrence Hunter, PhD., National Library of Medicine, Bldg. 38A, MS-54, Bethesda. MD 20894 (301) 496-9300 hunter@nlm.nih.gov (internet)

### \$150 printer hangs \$0.5M VAXcluster

Marc Shannon <R602MS5U@VB.CC.CMU.EDU> Tue, 9 Jun 92 14:36:21

Most people tend to enjoy their days off, Memorial Day included. Unfortunately, I received a call from our Operations staff at 4:30 in the morning on Memorial Day.

It seems that during their normal nightly backups, one of the systems seemed to have a problem. During processing of one of the disks, nothing happened -- the tape drive wasn't spinning and any attempt to exit out of the command (using ^Y) was ignored except for a useless "\*INTERRUPT\*" message on the console.

In frustration, they accidentally hit ^P which halted the system and then attempted to reboot. The system just would not come back up.

Something I should note about this system is that it (probably incorrectly) has the key "votes" for the VAXcluster to continue operating normally. Since it was down, all the other systems were waiting for it to come back up ("quorum lost, blocking activity").

After spending an hour fruitlessly searching for the problem, it turned out that the disk that the system had tried to backup had gone south. This disk was (incorrectly) single-ported to a single HSC (Hierarchical Storage Controller). The HSC's action to disk problems it to spit out the errors onto its console. The console had a locally attached printer which had run out of paper.

So, since there was no paper in the printer, the console hung waiting for it. Since the console was hung, the HSC waited for it. Since the HSC was hung, the VAX couldn't come up. Since the VAX couldn't come up, the VAXcluster wedged.

This is how a \$150 printer could hang a half-a-million dollar VAXcluster.

Sigh.. --Marc

# Reviewing Communications in the Gulf War

James Paul <jpaul@nsf.gov> Tue, 09 Jun 92 14:01:44 EDT

The following are excerpts from the article "The Data Weapon" [Peter Grier, in \_Government Executive\_, June 1992, p. 21], discussing U.S. communications support during the Iraqi conflict:

"...Throughout the Gulf theater of operations, satellite communications uplinks seemed as common as the crushed water bottles that littered allies' camps.... The ubiquitous dishes were visible evidence of the vast command, communications, control and intelligence (C3I) network the United States laid....

Getting it all working wasn't always easy. The communications network often needed workarounds and quick fixes to patch together equipment of different technical generations, with different software interfaces and protocols.

One big glitch occurred early on. In September 1990, it became apparent that the new Defense Switched Network was experiencing a horrible call-completion rate back to the United States, with only 20 to 30 percent of attempts going through. It took a troubleshooting effort of almost three months, involving AT&T and GTE technicians as well as military communicators, before the trouble was found: a signaling incompatibility between tactical and fixed systems. Over a three-day weekend, Bell Labs finally produced a new software patch to connect the systems, raising the call-completion rate to about 90 percent.

Another problem arose because the Army's new Mobile Subscriber Equipment communications switches had not yet been tested for operability with the older switches of the other services. The Joint Tactical Command, Control and Communications Agency back in the States had to whip up software fixes enabling the Army's switches to work the Marine/Air Force Unit Level Circuit Switch, as well as the French RITA communication system. This took 17 days, according to a DISA [Defense Information Systems Agency] report.

Meanwhile, the demand for connectivity was so great that DoD communicators were involved in an almost continuous search for all possible means of carrying messages [earlier in the report Grier mentioned that the daily message load was 700,000 telephone calls and 152,000 messages]. Among other things, the amount of electronic data being sent back and forth for tactical reasons was larger than anyone had ever envisioned.... Every time a new [satellite] came on line, it was used up."

\_Government Executive\_ is published by the same folks who put out the political magazine \_National Journal\_, and it's aimed at the inside-the-Beltway managerial crowd. One wonders what might have occurred had the Iraqis pursued a more rigorous electronic warfare strategy. "Interoperability" is still the big problem -- the Navy's inability to read the Air Force's computer-generated Air Tasking Order [the daily air war plan] is becoming almost as famous as the 82nd Airborne trooper who used his AT&T Calling Card to call Fort Bragg from Grenada, asking them to call the Navy because he couldn't get through on the

radio to ask the ships offshore for fire support (I'm going to be \_really\_ disappointed if that story turns out to be apocryphal). It also seems Patriot batteries could receive data from the Airborne Warning and Control System (AWACS) only with difficulty due to incompatible data links.

Typing errors are the fault of the contributor, not the magazine.

#### ✓ Endeavor bug -- more details

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Tue, 09 Jun 92 22:53:24 -0700

>From Aviation Week as quoted by James Paul:

Engineers have traced the problem to the sensitivity of NASA-developed equations to a particular set of numeric values that arose when Endeavour was making one of the final computer-targeted rendezvous maneuvers. Test show the software had been properly coded by IBM and therefore passed all preflight tests, according to Ted Keller, senior technical staff member at the IBM Shuttle Project Coordination Office, Houston.

Here is some additional information about this event. You can evaluate it yourselves with respect to the statements in AW.

The STS-49 failure of the flight software to converge during targeting has been traced to the Lambert targeting routine. The associated algorithms used by the routine converge on an independent variable called "U" which is a double precision scalar. U is iterated (up to 10 times) via this algorithm. The algorithm is designed to converge on a value of U between two dynamically updated limits called U\_MIN and U\_MAX, which are single precision scalars. On each iteration, either U\_MIN or U\_MAX is updated to decrease the interval within which the algorithm will search for the desired value of U.

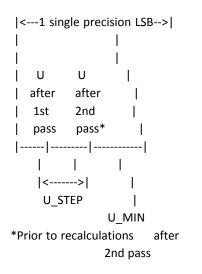
To determine which limit to update, the algorithm calculates a variable U\_STEP, the amount by which U will be updated on this iteration. If its value is positive, U\_MIN is set to U. If its value is negative, U\_MAX is set to U. Then U\_STEP is added to U, and the resulting value of U is compared to the limits U\_MIN and U\_MAX. If U is now outside the limits, U is recalculated as the average of U\_MIN and U\_MAX, thereby keeping U within the search interval.



U continues to be updated in this manner on each iteration until convergence is attained or maximum iterations are executed. Convergence occurs if the normalized transfer time that corresponds to the current value of U is close enough to the desired transfer time. "Close enough" is a function of a mission-specific data value.

For the third rendezvous of STS-49, the value of U after the first iteration was very close to the desired value, and U\_MIN was set equal to U because

U\_STEP was positive. On the second iteration cycle, U\_STEP was smaller thana one least significant bit (LSB) for U\_MIN. Since U\_STEP was positive, U\_MIN was set to U, and U\_STEP was added to U. Algebraically, U should have been greater than U\_MIN. However, due to precision differences, U\_MIN was greater than U. (Loss of precision occurred when the double precision value of U was stored into the single precision variable U\_MIN.) Therefore, U was recalculated to be the average of U\_MIN and U\_MAX, and the search interval no longer contained the desired value of U.



Note: both U and U-MIN had negative values

On subsequent iterations, U was updated in the direction of the desired value, but never reached it before maximum iterations occurred because it was outside the search interval.

To fix the problem and allow the mission to resume, they had to uplink a new state vector from the ground, by-passing the onboard routine. The permanent fix involves changing U\_MIN and U\_MAX to double precision.

### Where on earth are you?

Richard Murnane <richardm@runx.oz.au> Tue, 9 Jun 92 15:07:38 AEST

On Monday 8th June, I was tuning my amateur radio set across the 20-metre band, when I came across an emergency traffic net on 14.245 MHz. Several radio amateurs, in Hawaii, California, Florida, and Mexico City, were assisting an American marine vessel in the Carribean, the "Sea Harvest", whose navigation systems had been disabled, apparently by a lightning strike.

Miami Coast Guard was alerted and the Coast Guard cutter "Courageous" was dispatched from Jamaica to locate and assist the vessel.

One problem that arose was getting accurate coordinates for the vessel: all they had to go on was the last known LORAN readout from the previous day, and the direction and speed she had been sailing. Later, Sea Harvest contacted another ship on the marine distress frequency, VHF channel 16. Because Sea Harvest had a hand-held VHF tranceiver, the other ship would have been fairly close, and that ship's position reading would have been a reasonable approximation.

However, when it came to relaying that information to the Coast Guard, things became confused: the position was read out as "22 degrees, 34 minutes north, \*08 42 92\* West" (I don't recall all the digits correctly, but the longitude was read out as three pairs of digits).

The "08 42 92" was interpreted by all on frequency as being degrees/minutes/seconds, as most of us have been brought up to read geographical positions. The "08" was immediately rejected as a mistake, possibly in translation from Spanish to English, as 8 degrees west is in the Western Sahara desert, and it was judges that it was in fact \*80\* degrees West, which is in the Carribean. The ship which provided the coordinates however insisted that "08" was correct.

Several hours later, when authorisation was given to activate Sea Harvests's EPIRB (Emergency Positioning Information Radio Beacon), the longitude figure again came up as "084.."; it was only then that everyone realised that the first THREE digits represented degrees, and the remaining three the minutes in decimal format, eg 84 degrees 34.6 minutes.

The misinterpretation of the data format, when relayed over a voice radio link, led to a lot of confusion: one of the degree/minute/seconds coordinate groups placing the Sea Harvest five miles inland! This confusion lasted several hours until the EPIRB was activated.

I'm very suprised that the Coast Guard could have been caught out by this: It suggests that the "decimal minutes" representation is non-intuitive, or at least counter to the way most "non-mariner" people (e.g. the radio amateurs providing voice relays) have been educated to read geographical coordinates. (Or, perhaps, there are two different readout systems currently in use?)

Of course, when passing messages through one or more relay operators, one must be very careful not to try to "interpret" the message being passed, rather to send it \*exactly\* as received.

It also illustrates that even the most sophisticated, systems can fail, and that it's always best to have a safety backup. Presumably, Sea Harvest's HF radio antenna was on a different mast, and thus not destroyed by the lightning strike!

73 de Richard VK2SKY

### Kisk of Computer Generated Fund-Raising Letters

Lee Hasiuk <0003582947@mcimail.com> Tue, 9 Jun 92 17:49 GMT

>From a recently received Caltech Office of Annual Giving letter:

... Last year you gave \$0.00 to the Annual Fund. I would like to see you

increase your contribution this year by 25% or more if possible. ...

I can imagine the letter I'll get after I send them \$100:

... Thank you for being so generous by increasing your contribution from last year by Divide by 0 Core dumped

Lee Hasiuk, lee\_hasiuk@mcimail.com

#### Car computer downloading

<Bob\_Sidebotham@transarc.com> Tue, 9 Jun 1992 15:41:30 -0400 (EDT)

I have a new '92 Saturn SL with a computer controlled ignition system. I've been having some minor problems with cold start--sometimes after starting the car, the car seems to "hunt" for a good fast idle speed. It slow's the engine down until the RPM's reach zero and the car is about to stall, then suddenly boosts the engine speed to about 2000 RPM. Then it repeats.

The Saturn service manager mentioned that there is a software change due out at the end of the month. Saturn HQ will download this change to each dealership (by satellite link, I believe), and then each car will receive the software the next time it checks in for servicing. This is likely related to my problem.

There's all sorts of potential risks here, and no doubt many of them have been raised in this forum before. The important point is that the car I drive in to the service center is not the same car that I drive out! Prototypes of the car may have been driven for N million miles at proving grounds, but it didn't have the same software. How extensively has the software been tested? What are the security measures, if any, to ensure that the software I get is the software distributed by the factory? Do I have the option of not accepting the new software? I wonder if it's crossed anyone's mind that only downloading to selected cars would be a way of performing economical field tests on large numbers of cars (at some risk to those owners)? Even if this isn't explicitly intended, it works out that way since not all the cars are downloaded simultaneously--not yet, anyway.

As a sidenote, when you check in for Saturn service, your car's history is also uploaded to Saturn HQ. Every engine stall, my salesman told me, is recorded, as is the entire service history for each vehicle.

Bob Sidebotham, Transarc Corporation

# ✓ Telecom Australia allows easy denial of service attack

<[anonymous]> Wed, 10 Jun 92 12:22:14 xxT

I was dismayed to find out today that Telecom Australia (which holds

a virtual monopoly on telecommunications in this country) will disconnect a line given only two pieces of information:

- \* telephone number
- \* subscribers name

Anyone listed in the phone book, therefore, is an easy target for "prank" denial of service.

More seriously, however, are some of the technology related considerations. The building in which I work has a number of outside lines on a rotary. The alarm system when triggered, however, notifies a security firm on a fixed line. A high-tech criminal could simply have that line disconnected and we would never know (since the other lines on the exchange would still work).

There are two morals to the story. Firstly, the old problem of bureaucracies not validating requests is still alive and well. Secondly, the shortcoming of yet another automated system (our alarm) is highlighted when examining the TOTAL environment.

How many mission critical telecommunications users verify the internal checks and policies of their service provider?

### Follow-up to Dead Driver story -- PennDOT replies

Mike Berman <berman@gboro.glassboro.edu> Wed, 10 Jun 92 09:30:30 -0400

The following appeared on the letters page, Philadelphia Inquirer, Wednesday, June 10, 1992:

The rest of the story

Your story relating Eugene F. Smith's troubles with the Pennsylvania Department of Transportation (June 2) was not a complete representation of Mr. Smith's dealings with us. I'd like to offer your readers the rest of the story.

When we received a police report that Mr. Smith had been killed in a car accident, we edited his driving record accordingly. When Mr. Smith learned of the mistake to his record -- after the police stopped him for a driving violation -- he wrote to us, and we corrected his record and issued him a photo identification card since he was not eligible for a driver's license.

State law prevents me from disclosing any violations on an individual's personal driving record, so I cannot explain to you why a driver may be suspended or for how long. I can tell you that an indication on our record that a driver is deceased would in no way lead to a suspension. [comment --- special zombie permit?] I can also tell you that the rest of Mr. Smith's problems with Penn-DOT are because of his own disregard for state traffic safety laws.

I have asked the Pennsylvania State Police to investigate Mr. Smith's case so that it can be settled correctly as the law provides. Within those legal

parameters, we will work carefully with Mr. Smith to ensure that he understands his responsibilities to drive legally in Pennsylvania.

Howard Yerusalim, Secretary of Transportation, Harrisburg

# Ke: BBS Fraud (Lawson, <u>RISKS-13.56</u>)

Fred Gilham <gilham@csl.sri.com> Tue, 9 Jun 92 11:36:12 -0700

Another moral:

[...]

- 6) 'For Sale' notices for PC's etc. at low prices are posted from the stolen accounts.
- 7) Victims replying to the postings are requested to transfer money into the bogus bank account.
- 8) The money is withdrawn and the victims are out of luck.

[...]

Morals of this story:

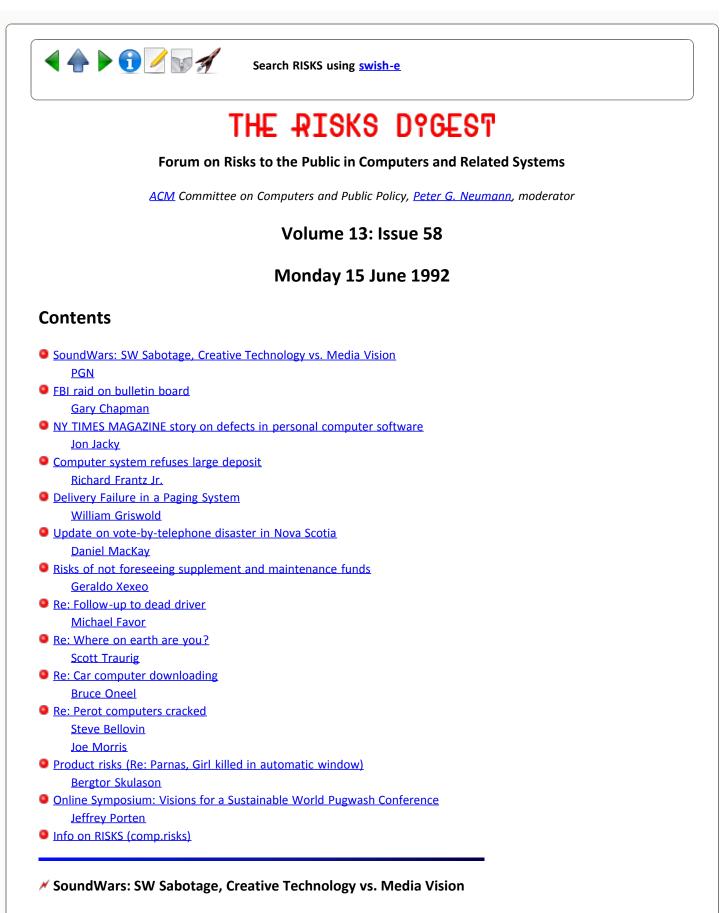
- A) Use different passwords for different accounts.
- B) Log on regularly to check for irregularities.
- C) When buying things advertised by computer, use COD.

-Fred Gilham gilham@csl.sri.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"Peter G. Neumann" <neumann@csl.sri.com> Fri, 12 Jun 92 10:07:17 PDT Creative Technology makes Sound Blaster, a sound board used by IBM compatibles to create game noises and other sound effects. Media Vision, Inc. develops computer peripherals and also makes a competing Thunder Board, designed to be compatible with software commonly used with Sound Blaster. However, a new release of a developer's software apparently works fine with Sound Blaster, but not with Thunder Board. Media Vision claims Creative Technology inserted a crash code that disables Media Vision's product, and has sued them for restraint of trade, unfair competition, and monopolization. (Media Vision was sued LAST MONTH by Creative Technology for violation of copyrights.) [Source: Article by Pamela Burdman, San Francisco Chronicle, 12 June 1992, p.B1]

[Sounds like the Suit-of-the-Month Club. Everyone seems to be joining. By the way, your media vision of RISKS is going to be creatively and technologically sporadic for a while as we observe Summer Slowdown Time. New subscribers should not be surprised if the traffic is light. PGN]

### FBI raid on bulletin board

Gary Chapman <chapman@silver.lcs.mit.edu> Thu, 11 Jun 92 10:30:37 -0400

Summarized from \*The Boston Globe\*, June 11, 1992, page 39:

The FBI raided the home of a computer bulletin board operator in Millbury, Massachusetts, yesterday, confiscating "several" computers, six modems, and a piece of equipment called "PC Board," which the FBI said was used to run the bulletin board system. The Software Publishers' Association brought the bulletin board to the FBI's attention, claiming that the system, called "Davy Jones' Locker," contained pirated copies of copyrighted software that users were encouraged to download. SPA claimed that there were over 200 different programs on the system, and users who uploaded copies of copyrighted software got free log-on time as a bonus. The alleged operator of the bulletin board, Richard Kenadek, was not arrested. The FBI would not comment on the case.

An SPA spokesperson said that the system had nearly 400 subscribers paying \$49 for three months or \$99 for a year to gain access to downloadable copies of Lotus 1-2-3, Microsoft Word, and other programs. SPA estimated that the system distributed \$675,000 worth of software since March of this year.

Sanford Sherizen, a computer security specialist in Natick, was quoted as saying, "We're making legal history here," because this case is apparently the first time federal authorities have gone after a bulletin board system for violations of copyright law.

The SPA representative said that the organization runs a telephone hotline for reports on bulletin boards offering downloadable copyrighted software, and they get "at least ten calls a day." SPA takes action against about two bulletin boards a week, usually with the threat of a lawsuit.

Gary Chapman, Coordinator, The 21st Century Project, Computer Professionals for Social Responsibility, Cambridge, Massachusetts chapman@lcs.mit.edu

# M NY TIMES MAGAZINE story on defects in personal computer software

Jon Jacky <JON@gaffer.radonc.washington.edu> Mon, 15 Jun 1992 9:11:47 -0700 (PDT)

This week's Sunday New York Times Magazine has a story by James Gleick, "Chasing bugs in the electronic village," (June 14, 1992, p. 38 ff). It describes users' experiences with the Microsoft Word for Windows product, as reported in a Compuserve forum and at user's group meetings. Gleick reports that, through several successive product versions, the vendor did not fix defects that were reported by many users and claimed the product included features that were incompletely and incorrectly implemented. Gleick also says these problems were not much reported in reviews in the trade magazines, even though they were widely known in the user community.

- Jon Jacky, Radiation Oncology RC-08, University of Washington, Seattle 98195

# ✓ Computer system refuses large deposit

"Richard Frantz Jr." <72570.2264@compuserve.com> 14 Jun 92 06:57:14 EDT

A branch bank officer told me that they had to refuse to accept deposit of a check for \$200,000 because the software, used by several banks in the area, couldn't handle more than \$99,999.99 in the deposit field. She insisted it was a computer error even though I tried to explain it was a specification error.

Richard Frantz Jr.

# ✓ Delivery Failure in a Paging System

# William Griswold <wgg@cs.UCSD.EDU> Mon, 15 Jun 92 16:32:19 PDT

I have a friend who is a clinical psychologist specializing in crisis counseling. Last weekend one of her patients was in an auto accident and called the counseling center hotline to ask for my friend. The patient's record indicated that her behavior could be self-destructive under stress. Following clinic procedure, the clinic (1) paged my friend. After a 10 minute wait for a call back they (2) paged her again. After another 10 minutes they (3) called her home, reaching her immediately. Her pager had been on and the batteries were fine, but it had not received the page. Anyway, my friend immediately called the patient to discover that she had taken a large dose of pills perhaps 30 minutes earlier. An ambulance was called and the woman was (barely) saved.

My friend's reaction to this failure was to update the patient's record specifying special handling procedures in the case of a crisis call. She rather blithely accepted the paging system failure and said that it happens all the time: phantom pages, missed pages, etc. Some of these are due to keying errors by the caller, others are due to environmental conditions blocking the radio signal. This incident is likely neither; two pages were made and my friend has never missed a page at home before.

Here are my questions:

- What are the failure modes of pager systems? For example: Can the system detect that a page is not getting through? What range of causes are there for a failed page? Can the person initiating the page be notified of failure?
- 2) What responsibilities does a paging service have to inform its users of failures as soon as it can detect them? What responsibility does it have to inform its users of recent failure rates?

BTW, The location of this incident was not in a metropolitan area. This means, apparently, that this paging service has a monopoly.

Bill Griswold, University of California, San Diego Dept. of Computer Science and Engr. wgg@cs.ucsd.edu

# ✓ Update on vote-by-telephone disaster in Nova Scotia (<u>RISKS-13.56</u>)

Daniel MacKay <daniel@nstn.ns.ca> Mon, 15 Jun 92 10:27:45 ADT

This is a follow-up on the huge local vote-by-phone fiasco. In <u>RISKS-13.56</u> I wrote about the vote-by-phone system contracted from the telco by the Liberal Party for their leadership convention, following Murphy's Law.

On June 8th, the telco held meetings with the Liberal Party, and with the media. As always, there's a little second guessing to do about what the press releases mean. Here's what they \*say\*:

- The system was composted of two software packages which had never been tested together at high call volume. ``All I can say, is it never occurred to anybody in my staff, and it never occurred to me.'' said Colin Lantham, the vice-president of business services for Maritime Tel and Tel.
- The first part of the system [presumably the touchtone answering /selection system] was capable of handling 78,000 calls an hour.
- The second part of the system, "set up to receive the caller's 8-digit PIN" proved much slower. [I'd guess that this was the interface to the databases that kept track of votes and who had voted. -dm]

The \*first\* part of the system had a dead-session detection function, to keep people from tying up phone lines. However, when the second part of the system started to slow down [transactions queued up? -dm] the first module hung up

before the second part issued an acknowledgement.

Also, the telco says when voting was restarted, ``some rogue information stayed in the system, causing some voters to be rejected." [They didn't reset the who-had-voted list, perhaps? -dm]. On the day of the fiasco, the telco initially blamed the problem on a missing line of code in the software, but they say now that that was a mistake. The problem of people being able to vote twice hasn't been mentioned.

The telco says the Liberal Party won't be charged for the services rendered on Saturday. [Like the power utility burning down your house with a million volts by accident, and saying ``Don't worry, you won't be billed for the electricity." -dm]

150 telco employees were recruited to test the system, [compared to 8000 voters in the real system! -dm] on Thursday the 11th, and it apparently worked. The telco reduced the number of incoming lines to cut down on system load.

The Liberal Party has decided to have another go at the vote-by-telephone system in a few days, but there won't be another convention. The telco will be posting a 350,000\$Cdn performance bond on the system, and there will be a paper-ballot backup system on hand.

Sme candidates have asked the telco for partial reimbursements of their campain costs on the basis that disclosure of the numbers (leaked via the kid with the scanner listening to the cellular conversations) have destroyed their chances of winning. The telco claims that the numbers leaked (numbers of calls recorded to each of the candidate's phone number) bear no relationship to the number of votes that had been collected or would have been collected.

Daniel MacKay, NOC Manager, NSTN Operations Centre, Dalhousie University, Halifax, Nova Scotia, Canada 902-494-NSTN daniel@nstn.ns.ca

#### Kisks of not foreseeing supplement and maintenance funds

Geraldo Xexeo <xexeo@dxlaa.cern.ch> Thu, 11 Jun 1992 13:58:21 GMT

I was very impressed by Mr. Shannon's message of a \$150 printer hanging up a \$0.5M VAXcluster (<u>RISKS-13.57</u>). Meanwhile, it reminded me a common "hang-up" problem we have in my institution (Federal University of Rio de Janeiro - Brazil).

It's reasonably easy for us to get money to buy hardware; actually, we have an ever-growing Sun and IBM-PC network. But, it is difficult to get money to buy supplements. This means that we are usually working under bad conditions, because of:

- 1. lack of paper or toner for our printers
- 2. lack of tapes to do backup
- 3. lack of maintenance contracts, due to lack of funds, etc...

It can be a third-world problem, but it is really a risk to invest in an expensive system if you cannot afford its maintenance. It can happen that the cheapest choice turns to be just wasted money.

Geraldo Xexeo, CERN - PPE Division, 1211 Geneve 23, Switzerland xexeo@dxlaa.cern.ch gxexeo@cernvm.bitnet FAX: (41) (22) 785 - 0207

#### Ke: Follow-up to dead driver (Berman, <u>RISKS-13.57</u>)

Michael Favor <favor@ecst.csuchico.edu> Wed, 10 Jun 92 19:40:08 pdt

How can Howard Yerusalim, State Secretary of Transportation, miss the point so completely while claiming to offer us the "rest of the story"? He accepts the fact that an anonymous driver was killed in a car accident while in possesion of Mr. Smith's stolen driver's license, yet completely ignores Mr. Smith's claim that the anonymous driver was also responsible for the traffic violations which caused the license to be suspensed.

I am not comforted by Mr. Yerusalim claims that State Law prohibits him from from disclosing details of an individual's driving record, when he then accuses Mr. Smith of vague and sweeping "disregard for state traffic safety laws" in a public newspaper. If Mr. Smith is cleared by the police investigation, will he sue the state for lost wages, related damages, and slander? It might help motivate Pennsylvania to correct the situation.

Perhaps some RISKS readers know what procedures are used by other state transportation departments to prevent similar situations, or could this happen to you?

Michael Favor, favor@csuchico.edu

### Ke: Where on earth are you? (Richard Murnane, <u>RISKS-13.57</u>)

Scott Traurig <traurig@ncavax.decnet.lockheed.com> Thu, 11 Jun 92 08:54:24 EDT

> I'm very suprised that the Coast Guard could have been caught out by this: It
 > suggests that the "decimal minutes" representation is non-intuitive, or at
 > least counter to the way most "non-mariner" people (e.g. the radio amateurs
 > providing voice relays) have been educated to read geographical coordinates.
 > (Or, perhaps, there are two different readout systems currently in use?)

Having raced "the big boats" for 9 years or so now, primarily as navigator, I may be able to supply a little background information here. With the advent of reliable and relatively inexpensive Loran navigational equipment, decimal minutes has become a very popular "readout system" for displaying position.

Most, if not all, units allow the user to select either degrees-minutesseconds or degrees-minutes-decimal minutes for display. Most users opt for the decimal minutes display. It is usually easier to plot to the nearest tenth of a minute, it is usually sufficient accuracy (approx. 200 yards - depends on latitude), and Loran isn't much more accurate than that for absolute position anyway. I do because all of my racing marks have been measured and listed in this manner by the local racing association, probably because of the above reasons. GPS units provide increased accuracy, of course, but 200 yards is usually plenty close most of the time. It is not unusual for a powerboat with a Loran or GPS coupled autopilot to collide with the buoy selected as a waypoint by an inattentive skipper.

I am also surprised that the Coast Guard couldn't figure it out. At the very least, the previous day's position would make it obvious, and the leading zero would make me suspicious.

Scott (traurig@ncavax.decnet.lockheed.com)

#### Ke: Car computer downloading (Sidebotham, <u>RISKS-13.57</u>)

### Bruce Oneel <oneel@arupa.gsfc.nasa.gov> Thu, 11 Jun 92 11:09:07 EDT

>As a sidenote, when you check in for Saturn service, your car's history is also >uploaded to Saturn HQ. Every engine stall, my salesman told me, is recorded, as >is the entire service history for each vehicle.

Hmm, how 'bout every engine overspeed (or overrev)? Or, since I suspect the engine knows what gear the transmission is in, how 'bout %time over 65mph? I can see it now. "I'm sorry, Mr Foo, but we show that you drive this car outside of it's limits. We can't do any warranty sevice because of this"

When engine computers were newer, I read in Car and Driver that Cadillac's new engine computer would record overspeeds. The person they were talking to implied that this might be used later if you reported engine problems.

Bruce O'Neel, NASA/GSFC/STX/Code 664 oneel@heasfs.gsfc.nasa.gov

#### Ke: Perot computers cracked

Steve Bellovin <smb@ulysses.att.com> Wed, 10 Jun 92 20:31:32 EDT

There were actually several reassuring things about the Perot incident, especially as per the full AP story. First, of course, they did have backups. Not only that, the backups were stored off-site. Second, the spokesperson said that they didn't store sensitive information on that machine, because too many people had access to it. Finally, he implied that the level of computer security wasn't that high, precisely because anyone, from anyone else's campaign, could have walked in off the street and achieved a position of trust. In other words, don't worry about your technical security measures if your other protections, including personnel screening, don't match up. Security is as strong as the weakest link, not the strongest. --Steve Bellovin

# Ke: Perot Computers Hacked (Hunter, <u>RISKS 13.57</u>)

Joe Morris <jcmorris@mwunix.mitre.org> Thu, 11 Jun 92 11:19:21 -0400

One of the local radio stations broadcasting the report of this incident noted that the Perot office had been staffed over the weekend with untrained \*and unsupervised\* volunteers. The broadcast drew no conclusions from this statement, but it strongly suggests that the problem may have the result of an innocent mistake in a poorly organized activity.

While it may in fact be somebody's deliberate attempt at sabotage, I'm more inclined at this point to agree with the old adage that one should not ascribe to malice anything which can be explained by simple stupidity. (On the other hand, this \*is\* a political environment, in which most rules are stood on their heads...)

Joe Morris

[There was also a related comment from Bill Bauserman, william.d.bauserman@gte.sprint.com]

# Product risks (Re: Parnas, Girl killed in automatic car window)

Bergtor Skulason <bergtor@ifi.uio.no> Mon, 15 Jun 1992 15:13:25 +0200

In RISK Volume 13 Issue 55, David Parnas writes:

> Isn't it just like our technocratic society to react to such an accident,

> caused by a completely unnecessary luxury becoming too complex, by making it

> even more complex? Wouldn't the simpler solution be to ban automatic windows

Integrating new technology into society is never painless. There is constant conflict between pressure for new technology (or new features) and need for stability. New technology causes changes no one can foresee, even less control. There is no easy solution. Public debate involving specialists, interest groups and lay people, and economic pressure on those "responsible" seems to be the least bad way of "controlling" technology.

Banning products usually harms the consumer more than protects him. Banning specific products or features can be feasible in clear cut cases, but cases usually are not clear cut. If they are, we usually have a case for product liability not a ban. Value of products can never be stated objectively. Its always relevant to a person or a group. What is useless to some does have value for others. (Very few things, if any, can be shown to have objective value independent of a person or a group).

Complex regulations on safety usually lead to more complex products, that are more expensive and more error prone. And worse it releases producers from responsibility, because they can refer to the regulations.

There is a conflict between government intervention and freedom. To much or too little harms the public, not the producers. Through public debate and by placing (economic) responsibility were its possible, pressure can be built to

increase product quality and safety. Under pressure products become simpler and safer, and their price reflects the producers risk of producing, because he can not put that risk anywhere else.

Private replies to: B. Skulason, Univ. of Iceland, beggi@rhi.hi.is

✓ Online Symposium: Visions for a Sustainable World Pugwash Conference

Jeffrey Porten <porten@eniac.seas.upenn.edu> 14 Jun 92 04:58:45 GMT

CALL FOR PARTICIPATION VIA ELECTRONIC MAIL

STUDENT PUGWASH USA SEVENTH BIENNIAL CONFERENCE ON SCIENCE, TECHNOLOGY, AND SOCIAL RESPONSIBILITY

VISIONS FOR A SUSTAINABLE WORLD Emory University, Atlanta, Georgia June 14-20, 1992

The Student Pugwash USA Biennial Conference assembles ninety students from around the world for a week-long conference to address the impact of science and technology on society. The students will join accomplished men and women from science, government, industry, and academe for an intensive week of discussion and interaction focusing on the following issues:

- Environmental Challenges for Developing Countries
- Energy Options: Their Social and Environmental Impact
- Health Care in Developing Countries
- Changing Dynamics of Peace and Global Security
- Educating for the Socially Responsible Use of Technology
- Ethics and the Use of Genetic Information

We are inviting all members of the e-mail community to take part in an online symposium discussing the topics at the conference. Each day, a summary of the plenary and working group discussions will be mailed out as soon as possible following their completion. Participants in the online symposium are invited to send back their replies, commenting on what you receive. Copies will be redistributed back through electronic mail, and printed and used at the conference. Of course, you're welcome to sign up for the mailings even if you won't have the time to participate.

If you are interested in participating, send e-mail to

porten@eniac.seas.upenn.edu. You will be sent more information about Student Pugwash USA, and will receive all conference summaries. Feel free to subscribe anytime during the conference, or even after it's over, as all messages will be archived and can be sent out at any time. Please include in your message your full name; we would also appreciate if you include your current occupation (or student affiliation), and your city, state, and country, but this is optional.

You can also call the Student Pugwash electronic bulletin board at

215/898-2019, for more information about Student Pugwash, and to participate in ongoing discussion about the impact of science and technology on society. Feel free to write me, as well, if you have any specific questions.

Student Pugwash USA is a non-partisan, non-profit organization with chapters at 35 colleges and high schools across the country. Sister Student/Young Pugwash organizations exist in 20 countries on four continents. For more information, reply to this message at porten@eniac.seas.upenn.edu.

More information about the conference follows.

For each of the listed topics, student and senior participants form small working groups in which they will meet every morning throughout the conference week to discuss areas of mutual interest and expertise. These intensive discussions offer an invaluable opportunity for students to explore the ethical and value questions posed by advances in science and technology with forward-thinking professionals.

Senior Participants will be present from the U.S. Congress, National Institutes of Health, National Academy of Sciences, Carter Center, Centers for Disease Control, Brookings Institution, Emory University, and many other prominent institutions. Several special events will also be held, including a day at the Carter Presidential Center in Atlanta and an interactive, multi-media World Game Workshop.

The separate working group meetings are complemented by afternoon and evening plenary sessions for the full conference. Plenaries will address issues which cut across disciplinary boundaries such as ethical conduct in scientific research, race and gender in science, technology and global responsibility, and religion and science.

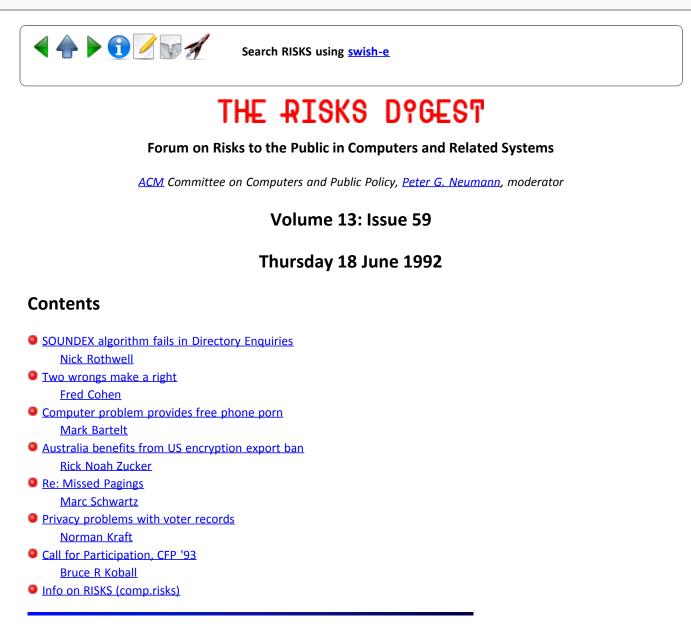
Student Pugwash USA is committed to representing a broad spectrum of political, international, and disciplinary perspectives. Previous conferences have attracted participants from over thirty nations. We are striving for even greater international, intergenerational, and interdisciplinary representation at the 1992 conference.

Jeff Porten, Annenberg School for Communication, UPenn Graduate Group in American Civilization, UPenn



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# SOUNDEX algorithm fails in Directory Enquiries

Nick Rothwell <nick@dcs.edinburgh.ac.uk> Tue, 16 Jun 1992 10:45:55 +0000

This is something I picked up while having some discussions at a software company here in Edinburgh. The company has a Gaelic name, and has been having problems with British Telecom's directory enquiries service not finding their entry. Apparently, all calls to directory enquiries are put through an implementation of the SOUNDEX algorithm: the operator listens to the name given by the caller, and types in the name as heard or a close phonetic approximation to it. I don't know a great deal about SOUNDEX, but it doesn't work for Gaelic, even though the company's name (An Teallach) is not too distant from the phonetic pronunciation (An Chellack).

The final part of the long, heated discussion with the BT engineer revealed that they've been having a lot of problems with the system, especially with people calling up to ask for phone numbers of French restaurants...

Nick

### Two wrongs make a right

fc <FBCohen@DOCKMASTER.NCSC.MIL> Wed, 17 Jun 92 14:55 EDT

Those of us who are aware that denial results when the output queues for peripherals overrun are aware that it can be devastating, but there are also those of us who take advantage of it as if it were a feature. Here is what happened to me today.

On a 3B2, the system backups and restoration program does not allow you to restore information to different directory structures than it was backed up from without great difficulty. I happened to have over 9,000 files to restore to a system, and they were backed up from "/v", but the system they were being restored on had only a "/u" it would fit on. (These are Unix sub\directories). As a result, I essentially had to do the restore to a newly created "/v" in the root file system, which did not have enough file space available to do the entire restore. I had a plan - As the tape was restored, I would copy disk-to-disk and delete the incoming files after copying them. I have done this "race" before, and I knew that I had to transfer out at a rate high enough so that the root file system would not overrun - which is to say, I had to beat the incoming tape transfer with disk to disk transfers. Of cours the tape in streeming mode operates faster than the disk I was using, so in the end, it was helpless because it takes two disk accesses to move a file from one disk to another, but only 1 access to get a new file from the tape. I tried putting in multiple transfer processes at high priority, but of course, the DMAs always won from the tape to the disk.

The solution I used (when the available space began to get critical) was to halt output on the console! Hard to believe it works? Of course it does. The tape transfers produce a dot on the screen for each of the files transfered in, and by pressing <ctrl>s (stop output) I was able to block the tape transfer process after only a few hundred more files are transfered. By watching the disk space, stopping the console output to block tape transfers when space got too low, and continuing output when more space was created by the transfer to the second disk, I was able to complete the job.

The point of this insanity is that as a practical matter, there are times when knowing how to cause denial of services can be a very useful part of systems administration - especially when we can do it so selectively. The title of this piece indicates that by knowing about how to break a system, I was able to compensate for one flaw in the system by exploiting another flaw hence, 2 wrongs made a right!

P.S. I am interested in other stories where knopwn holes were used to compensate creatively for other known holes. It is my contention that most of the best systems administrators and systems programmers know about and exploit these sorts of things all of the time, and that without these flaws, we would

really have to design systems right - otherwise, we would never be able to make up for the wrongs with other wrongs.

FC

#### Computer problem provides free phone porn

Mark Bartelt <sysmark@orca.cita.utoronto.ca> Thu, 18 Jun 92 08:00:43 EDT

[Toronto Star, 17-Jun-92]

Bell attempts to correct error that allows free phone-sex calls

OTTAWA (CP) -- Bell Canada is scrambling to repair a computer error that allows some Ottawa pay phones to dispense free phone-sex services.

The error has been giving callers easy access for months to graphic recordings of simulated kinky sex. Callers have also been able to speak to women whose job is to fulfil sexual fantasies by talking dirty.

Bell officials weren't aware of the glitch in the system until an Ottawa Citizen reporter told them of it, said official Lynn Francoeur.

Phone-sex clients "certainly weren't going to call Bell and tell us they were getting this for free."

Francoeur could not say why Bell hadn't detected the error which has affected pay phones in Ottawa's west end and in the nearby community of Nepean. Nor could she say how much money Bell and the phone-sex companies have lost, or how long the error has existed.

Many west-end high school students have been in the know for months. At Woodroffe High School, where three pay phones allowed the no-charge calls, several teenagers said they knew of the free dial-a-porn since late 1990.

"It's perverted," said a 16-year-old male in Grade 10, who asked not to be identified.

Mark Bartelt	416/978-5619
Canadian Institute for	mark@cita.toronto.edu
Theoretical Astrophysics	mark@cita.utoronto.ca

#### Australia benefits from US encryption export ban

<noah@cs.washington.edu> Wed, 17 Jun 92 16:19:13 -0700

>From The Courier-Mail, Queensland, Australia - May 18, 1992 "Pay-TV boost to technology" (copied without permission)

A US export ban on pay-TV decoding technology could lead to a multibilliondollar, Australian-led revolution in the industry. The 15-year-old decoding or encryption system used in the US is classified "military sensitive", ruling out its export to and use in Australia when this country introduces a pay-TV system in 1994.

Far from creating a major hurdle for Australia's nascent pay-TV industry - pay

TV cannot work without a signal decoding system - the export ban is likely to result in a massive boost for Australian technology.

After three years of developmental work, Gold Coast-based electronics company Digital Blanking Systems has produced a pay-TV "black box" which, it says, is better than the American version and which could save Australia \$100 million a year in imports. [RNZ - \$A1 = ~\$US0.76]

The company says its revolutionary decoder could earn Australia up to \$2.5 billion a year in exports if the designed was accepted in key Asian and European pay-TV markets.

So, what we've said in the past about US export restrictions on encryption technology being detrimental economically is coming to pass.

Rick Noah Zucker, Dept. of Computer Science & Eng., University of Washington noah@cs.washington.edu

### Ke: Missed Pagings (<u>RISKS-13.58</u>)

<SchwartzM@DOCKMASTER.NCSC.MIL> Tue, 16 Jun 92 12:38 EDT

In the June 15 issue of <u>RISKS-13.58</u>, Bill Griswold of UCSD describes an incident that took place regarding a missed page that nearly cost the life of a person in personal crisis. I cannot comment on the availability of any type of fault-tolerance in most radio paging system, that is can the system confirm that the page was recieved by the intended beeper? It would seem that the beepers that are typically available cannot transmit a return signal to indicate reception. I make that statement based upon the logical assumption that if the system needs a 100 foot tall (sometimes taller) tower to transmit the primary signal to the pager, the pager does not have the power to send a return signal. There are certainly experts out there in radio signal transmission that can comment on the specifics. But in most cases, it takes less power to sense a transmission than to actually generate one. Automotive radar detectors are a prime example of this.

My personal experience has had similar events. In my former life as a cardiac surgical assistant, there were times that I missed pages during life threatening situations when patients were in need of immediate attention from a health care professional. I had a Motorola BPR2000 beeper (the LCD display type) that was considered one of the best at the time (1981 - 1986 time frame) and there were more times than I care to think about when I was either in the hospital or on call away from the hospital that pages were missed. In no case did anyone die (luckily), but it did create enormous amounts of tension as precious minutes were sometimes lost due to not recieving the page the first time. In one circumstance, I changed from the hospital's own system to a commercial system, that was significantly more reliable (higher power transmitter with a better, more central antenna location). With that system, I did not miss any pages over the course of the subsequent year. At least that I know of!

I also would be curious to hear of any similar experiences and any expert comments on the nature of error detection and correction on the systems, especially with the new nation-wide paging systems that are in wide spread use by companies, including my present employer for our field personnel.

Marc Schwartz, Director, Clinical Services, Summit Medical Systems Minneapolis, Minnesota E-mail: SchwartzM at dockmaster.ncsc.mil

#### ✓ privacy problems with voter records

Lance J. Hoffman <hoffman@seas.gwu.edu> Wed, 17 Jun 92 15:53:06 EDT

Date: Wed, 17 Jun 92 11:49:09 PDT From: "Willis H. Ware" <willis%iris@rand.org>

From: nkraft@bkhouse.cts.com (Norman Kraft) Newsgroups: alt.privacy Subject: Privacy alert:San Diego voters on CD Date: 8 Jun 92 18:31:33 GMT Organization: Argus Computing, San Diego, CA

An article that made the front page of the San Diego Union on Sunday, June 7, 1992 bore the title: "Technology pits privacy vs. Information Age". The article starts with these paragraphs:

#### +++++

The morning after Bill Turner voted in last week's election, he picked up a copy of a local computer magazine and his jaw dropped. "This ad just jumped out and hit me in the face," said the 35-year old La Mesa computer programmer. "It was a severe shock." There, for sale, were Turner's name, address, unlisted telephone number, occupation, birthplace, birthdate and political affiliation.

A list of San Diego County's 1.25 million registered voters containing the information is available for \$99 in a relatively new format [CD-ROM] that virtually anyone with a personal computer can use. It is the first known such use of voter registration data in the nation.

#### +++++

The CD-ROM is marketed by a San Diego company call Sole Source Systems, a local computer store.

Lists of voter information have always been available, and political campaigns have had access to the information on data tapes for years. This is, however, the first time that such information has been made available to the public at large, in an easily accessible format (dBase, from what I can gather).

Sole Source says that use of the CD is limited to "election purposes, ...election, scholarly or political research, or government purposes." Sole

Source says that they require ID and the completion of a form before selling the CD. Turner responds to this with "What is there to prevent me from going up there and telling him I'm with the Little Old Ladies Auxilliary 97, and I want this list to call people up and help arrange transportation to the polls on Election Day? It would be a bald-faced lie, but I would get it [the CD]."

He may be right, as Conny McCormack, the San Diego County Registrar of Voters says that the registrar's office does not check to make sure the list is being used within the law, primarily because "we have no authority in that area."

David Banisar, a policy analyst with Computer Professionals for Social Responsibilities in Washington, DC, said in all likelihood the CD would end up in the hands of direct marketers. "This is really an unanticipated use of the data," he said, "You register to vote because you want to feel patriotic and do your citizen's duty and try to get some good government. You don't register to vote so that you can be solicited by every bozo out there with a widget that he feels he should hock to you."

The article goes on to discuss the problems of privacy in the computer age, and mentions two other CD-ROM databases that are publicly available: PhoneDisc USA, from a corporation of the same name in Marblehead, Mass., lists 90 million names, addresses and phone numbers nation wide. MetroScan CD, from Transamerica Information Management in Sacramento, is a database containing housing ownership information, from deed filings, and for a given address provides the owner's name, address, when the building was purchased, how many bedrooms and bathrooms it has, how many square feet it has, and it's property tax assessment.

In the article, Ken Smith, from Transamerica Information Magagement, is quoted as saying:

"I'm very much in favor of making the information, if it's in the public domain, available to a very wide audience, rather than just major corporations and government agencies. It's a very, very powerful tool for the little guy."

and further:

"I don't think the privace issue has been a concern yet. I can see where it might be in the future, but it's not a problem now."

Finally the article goes back to Dante Tuccero, from PhoneDisc USA Corp., listing such PhoneDisc customers as "the U.S. Drug Enforcement Administration, the Navy, the Air Force, the Social Security Administration, as well as local libraries and law enforcement, public investigators, geneologists, and even high school and college reunions." Quoting Tuccero, "There's a company in Langley, Va,. that uses it, I believe, but wouldn't say so."

The last paragraphs of the article point out that "the direct-mail company that provides PhoneDisc with most of it's data prefers to remain off other people's lists."

"We're not at liberty to share that," Tuccero said, "A lot of data

providers like to be low key."

The saddest part of the whole article, in my opinion, is this statement from Turner: "I have voted in every election since I was 18, and I think (this) was the last election I'll ever vote in."

[For those concerned about the PhoneDisc listings, they will remove your name from the next release of their CD if you call. They claim that only two people have called so far. I imagine we can change that! Their number in Marblehead, Mass. as given by directory assistance, is 617-639-2900.]

Norman R. Kraft, Senior Partner, Argus Computing, San Diego, CA UUCP : ucsd!crash!bkhouse!nkraft INET : nkraft@bkhouse.cts.com

----- Message 2

From: jim@rand.org (Jim Gillogly) Newsgroups: alt.privacy Subject: Re: Privacy alert:San Diego voters on CD Summary: PhoneDisc won't remove names. Date: 9 Jun 92 21:18:44 GMT

•••

I called this number to get removed from their list. The lady who answered the phone was polite, and told me that they got their information from the white pages of phone books around the country, which are public information. I told her I wanted to be removed from their product, and she responded that all I needed to do was to get an unlisted number from the phone company so that I would not be in the next phone book, and that would prevent me from getting into the next copy of their product. They will not remove someone from it individually.

Looks like more cause for concern...

Jim Gillogly jim@rand.org

### Call for Participation, CFP '93

Bruce R Koball <bkoball@well.sf.ca.us> Tue, 16 Jun 92 19:28:55 -0700

CFP'93

The Third Conference on Computers, Freedom and Privacy Sponsored by ACM SIGCOMM, SIGCAS & SIGSAC 9 - 12 March 1993 San Francisco Airport Marriott Hotel, Burlingame, CA

#### INVITATION

This is an invitation to submit session and topic proposals for

inclusion in the program of the Third Conference on Computers, Freedom and Privacy. Proposals may be for individual talks, panel discussions, debates or other presentations in appropriate formats. Proposed topics should be within the general scope of the conference, as outlined below.

#### SCOPE

The advance of computer and telecommunications technologies holds great promise for individuals and society. From convenience for consumers and efficiency in commerce to improved public health and safety and increased participation in democratic institutions, these technologies can fundamentally transform our lives.

At the same time these technologies pose threats to the ideals of a free and open society. Personal privacy is increasingly at risk from invasion by high-tech surveillance and eavesdropping. The myriad databases containing personal information maintained in the public and private sectors expose private life to constant scrutiny.

Technological advances also enable new forms of illegal activity, posing new problems for legal and law enforcement officials and challenging the very definitions of crime and civil liberties. But technologies used to combat these crimes can threaten the traditional barriers between the individual and the state.

Even such fundamental notions as speech, assembly and property are being transformed by these technologies, throwing into question the basic Constitutional protections that have guarded them. Similarly, information knows no borders; as the scope of economies becomes global and as networked communities transcend international boundaries, ways must be found to reconcile competing political, social and economic interests in the digital domain.

The Third Conference on Computers, Freedom and Privacy will assemble experts, advocates and interested people from a broad spectrum of disciplines and backgrounds in a balanced public forum to address the impact of computer and telecommunications technologies on freedom and privacy in society. Participants will include people from the fields of computer science, law, business, research, information, library science, health, public policy, government, law enforcement, public advocacy and many others.

Topics covered in previous CFP conferences include:

Personal Information and Privacy International Perspectives and Impacts Law Enforcement and Civil Liberties Ethics, Morality and Criminality Electronic Speech, Press and Assembly Who Logs On (Computer & Telecom Networks) Free Speech and the Public Telephone Network Access to Government Information Computer-based Surveillance of Individuals Computers in the Workplace Who Holds the Keys? (Cryptography) Who's in Your Genes? (Genetic Information) Ethics and Education Public Policy for the 21st Century

These topics are given as examples and are not meant to exclude other possible topics on the general subject of Computers, Freedom and Privacy.

#### PROPOSAL SUBMISSION

All proposals should be accompanied by a position statement of at least one page, describing the proposed presentation, its theme and format. Proposals for panel discussions, debates and other multi-person presentations should include a list of proposed participants and session chair. Proposals should be sent to:

CFP'93 Proposals 2210 Sixth Street Berkeley, CA 94710

or by email to: cfp93@well.sf.ca.us with the word "Proposal" in the subject line. Proposals should be submitted as soon as possible to allow thorough consideration for inclusion in the formal program. The deadline for submissions is 15 August 1992.

#### STUDENT PAPER COMPETITION

Full time students are invited to enter the student paper competition. Winners will receive a scholarship to attend the conference and present their papers.

Papers should not exceed 2500 words and should address the impact of computer and telecommunications technologies on freedom and privacy in society. All papers should be submitted to Professor Dorothy Denning by 15 October 1992. Authors may submit their papers either by sending them as straight text via email to: denning@cs.georgetown.edu or by sending 6 printed copies to:

Professor Dorothy Denning Georgetown University Dept. of Computer Science 225 Reiss Science Bldg. Washington DC 20057

Submitters should include the name of their institution, degree program, and a signed statement affirming that they are a fulltime student at their institution and that the paper is an original, unpublished work of their own.

#### INFORMATION

For more information on the CFP'93 program and advance registration, as it becomes available, write to:

CFP'93 Information 2210 Sixth Street Berkeley, CA 94710

or send email to: cfp93@well.sf.ca.us with the word "Information" in the subject line.

#### THE ORGANIZERS

#### General Chair

Bruce R. Koball CFP'93 2210 Sixth Street Berkeley, CA 94710 510-845-1350 (voice) 510-845-3946 (fax) bkoball@well.sf.ca.us

Steering Committee

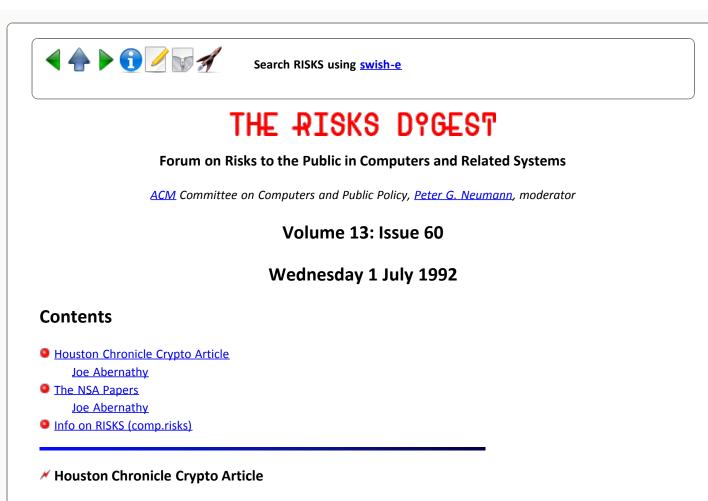
# ×

Mary J. Culnan David D. Redell		
Georgetown University DEC Systems Resea	rch	
Center		
Dorothy Denning		
Georgetown University Marc Rotenberg		
Computer Professionals		
Les Earnest for Social Responsibility		
GeoGroup, Inc.		
C. James Schmidt		
Mike Godwin San Jose State Universit	ty	
Electronic Frontier Foundation		
Barbara Simons		
Mark Graham IBM		
Pandora Systems		
Lee Tien		
Lance J. Hoffman Attorney		
George Washington University		
George Trubow		
Donald G. Ingraham John Marshall Law So	chool	
Office of the District Attorney,		
Alameda County, CA Willis Ware		
Rand Corp.		
Simona Nass		
Student - Cardozo Law School Jim Warren		
Microtimes		

Peter G. Neumann
& Autodesk, Inc.

SRI International

Affiliations are listed for identification only.
Please distribute and post this notice!
Image: Control of the contro



Joe Abernathy <Joe.Abernathy@houston.chron.com> Wed, 24 Jun 92 18:02:18 CDT

This cryptography article appeared Sunday, June 21. It is being forwarded to RISKS as a way of giving back something to the many thoughtful participants here who helped give shape to the questions and the article.

In a companion submission [see <u>RISKS-13.61</u>], I include the scanned text of the NSA's 13-page response to my interview request, which appears to be the most substantial response they've provided to date. I would like to invite feedback and discussion on the article and the NSA document. Please send comments to edtjda@chron.com

Promising technology alarms government --Use of super-secret codes would block legal phone taps in FBI's crime work By JOE ABERNATHY, Copyright 1992, Houston Chronicle

Government police and spy agencies are trying to thwart new technology that allows conversations the feds can't tap. A form of cryptography -- the science of writing and deciphering codes -- this technology holds the promise of guaranteeing true privacy for transactions and communications. But an array of Federal agencies is seeking to either outlaw or severely restrict its use, pointing out the potency of truly secret communications as a criminal tool.

"Cryptography offers or appears to offer something that is unprecedented," said Whitfield Diffie, who with a Stanford University colleague devised public

key cryptography," an easily used cryptography that is at the center of the fight. ``It looks as though an individual might be able to protect information in such a way that the concerted efforts of society are not going to be able to get at it. ``No safe you can procure has that property; the strongest safes won't stand an hour against oxygen lances. But cryptography may be different. I kind of understand why the police don't like it."

The National Security Agency, whose mission is to conduct espionage against foreign governments and diplomats, sets policy for the government on matters regarding cryptography. But the FBI is taking the most visible role. It is backing legislation that would address police fears by simply outlawing any use of secure cryptography in electronic communications. The ban would apply to cellular phones, computer networks, and the newer standard telephone equipment -- already in place in parts of Houston's phone system and expected to gain wider use nationwide.

``Law enforcement needs to keep up with technology," said Steve Markardt, a spokesman for the FBI in Washington. ``Basically what we're trying to do is just keep the status quo. We're not asking for anything more intrusive than we already have." He said the FBI uses electronic eavesdropping only on complex investigations involving counterterrorism, foreign intelligence, organized crime, and drugs. ``In many of those," he said, we would not be able to succeed without the ability to lawfully intercept."

The State and Commerce departments are limiting cryptography's spread through the use of export reviews, although many of these reviews actually are conducted by the NSA. The National Institute of Standards and Technology, meanwhile, is attempting to impose a government cryptographic standard that critics charge is flawed, although the NSA defends the standard as adequate for its intended, limited use.

``It's clear that the government is unilaterally trying to implement a policy that it's developed," said Jim Bidzos, president of RSA Data Security, which holds a key cryptography patent. ``Whose policy is it, and whose interest does it serve? Don't we have a right to know what policy they're pursuing?" Bidzos and a growing industry action group charge that the policy is crippling American business at a critical moment.

The White House, Commerce Department, and NIST refused to comment.

The NSA, however, agreed to answer questions posed in writing by the Houston Chronicle. Its purpose in granting the rare, if limited, access, a spokesman said, was ``to give a true reflection'' of the policy being implemented by the agency. ``Our feeling is that cryptography is like nitroglycerin: Use it sparingly then put it back under trusted care,'' the spokesman said.

Companies ranging from telephone service providers to computer manufacturers and bankers are poised to introduce new services and products including cryptography. Users of electronic mail and computer networks can expect to see cryptography-based privacy enhancements later this year.

The technology could allow electronic voting, electronic cash transactions, and a range of geographically separated -- but secure -- business and social interactions. Not since the days before the telephone could the individual

claim such a level of privacy.

But law enforcement and intelligence interests fear a world in which it would be impossible to execute a wiretap or conduct espionage.

"Secure cryptography widely available outside the United States clearly has an impact on national security," said the NSA in its 13-page response to the Chronicle. "Secure cryptography within the United States may impact law enforcement interests."

Although Congress is now evaluating the dispute, a call by a congressional advisory panel for an open public policy debate has not yet been heeded, or even acknowledged, by the administration.

The FBI nearly won the fight before anyone knew that war had been declared. Its proposal to outlaw electronic cryptography was slipped into another bill as an amendment and nearly became law by default last year before civil liberties watchdogs exposed the move.

"It's kind of scary really, the FBI proposal being considered as an amendment by just a few people in the Commerce Committee without really understanding the basis for it," said a congressional source, who requested anonymity. "For them, I'm sure it seemed innocuous, but what it represented was a fairly profound public policy position giving the government rights to basically spy on anybody and prevent people from stopping privacy infringements."

This year, the FBI proposal is back in bolder, stand-alone legislation that has created a battle line with law enforcement on one side and the technology industry and privacy advocates on the other. ``It says right on its face that they want a remote government monitoring facility'' through which agents in Virginia, for instance, could just flip a switch to tap a conversation in Houston, said Dave Banisar of the Washington office of Computer Professionals for Social Responsibility.

Though the bill would not change existing legal restraints on phone-tapping, it would significantly decrease the practical difficulty of tapping phones -- an ominous development to those who fear official assaults on personal and corporate privacy. And the proposed ban would defuse emerging technical protection against those assaults.

CPSR, the point group for many issues addressing the way computers affect peoples' lives, is helping lend focus to a cryptographic counterinsurgency that has slowly grown in recent months to include such heavyweights as AT&T, DEC, GTE, IBM, Lotus, Microsoft, Southwestern Bell, and other computer and communications companies.

The proposed law would ban the use of secure cryptography on any message handled by a computerized communications network. It would further force service providers to build access points into their equipment through which the FBI -- and conceivably, any police officer at any level -- could eavesdrop on any conversation without ever leaving the comfort of headquarters.

"It's an open-ended and very broad set of provisions that says the FBI can demand that standards be set that industry has to follow to ensure that (the FBI) gets access," said a congressional source. "Those are all code words for if they can't break in, they're going to make (cryptography) illegal. "This is one of the biggest domestic policy issues facing the country. If you make the wrong decisions, it's going to have a profound effect on privacy and security."

The matter is being considered by the House Judiciary Committee, chaired by Rep. Jack Brooks, D-Texas, who is writing a revision to the Computer Security Act of 1987, the government's first pass at secure computing.

The recent hearings on the matter produced a notable irony, when FBI Director William Sessions was forced to justify his stance against cryptography after giving opening remarks in which he called for stepped-up action to combat a rising tide of industrial espionage. Secure cryptography was designed to address such concerns.

The emergence of the international marketplace is shaping much of the debate on cryptography. American firms say they can't compete under current policy, and that in fact, overseas firms are allowed to sell technology in America that American firms cannot export.

"We have decided to do all further cryptographic development overseas," said Fred B. Cohen, a noted computer scientist. "This is because if we do it here, it's against the law to export it, but if we do it there, we can still import it and sell it here. What this seems to say is that they can have it, but I can't sell it to them -- or in other words -- they get the money from our research."

A spokeswoman for the the Software Publishers Association said that such export controls will cost \$3-\$5 billion in direct revenue if left in place over the next five years. She noted the Commerce Department estimate that each \$1 billion in direct revenue supports 20,000 jobs.

The NSA denied any role in limiting the power of cryptographic schemes used by the domestic public, and said it approves 90 percent of cryptographic products referred to NSA by the Department of State for export licenses. The Commerce Department conducts its own reviews. But the agency conceded that its export approval figures refer only to products that use cryptology to authenticate a communication -- the electronic form of a signed business document -- rather than to provide privacy.

The NSA, a Defense Department agency created by order of President Harry Truman to intercept and decode foreign communications, employs an army of 40,000 code-breakers. All of its work is done in secret, and it seldom responds to questions about its activities, so a large reserve of distrust exists in the technology community.

NSA funding is drawn from the so-called ``black budget," which the Defense Budget Project, a watchdog group, estimates at \$16.3 billion for 1993.

While the agency has always focused primarily on foreign espionage, its massive eavesdropping operation often pulls in innocent Americans, according to

James Bamford, author of \_The Puzzle Palace\_, a book focusing on the NSA's activities. Significant invasions of privacy occurred in the 1960s and 1970s, Bamford said.

Much more recently, several computer network managers have acknowledged privately to the Chronicle that NSA has been given access to data transmitted on their networks -- without the knowledge of network users who may view the communications as private electronic mail.

Electronic cryptology could block such interceptions of material circulating on regional networks or on Internet -- the massive international computer link.

While proponents of the new technology concede the need for effective law enforcement, some question whether the espionage needs of the post-Cold War world justify the government's push to limit these electronic safeguards on privacy.

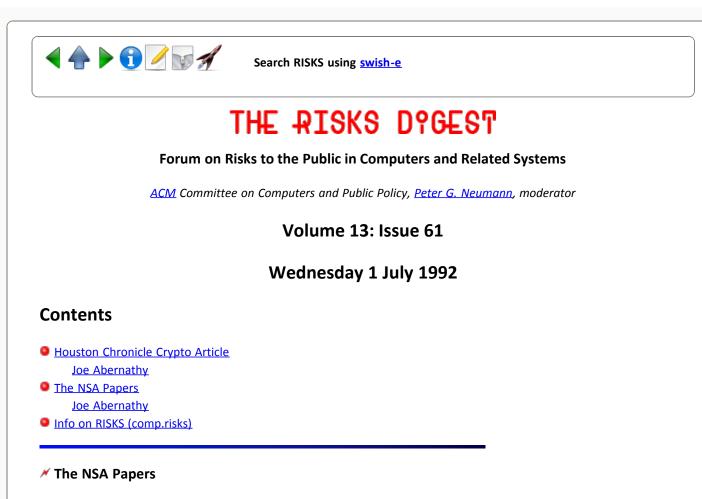
"The real challenge is to get the people who can show harm to our national security by freeing up this technology to speak up and tell us what this harm is," said John Gilmore, one of the founders of Sun Microsystems. "When the privacy of millions of people who have cellular telephones, when the integrity of our computer networks and our PCs against viruses are up for grabs here, I think the battleground is going to be counting up the harm and in the public policy debate trying to strike a balance."

But Vinton Cerf, one of the leading figures of the Internet community, urged that those criticizing national policy maintain perspective. ``I want to ask you all to think a little bit before you totally damn parts of the United States government," he said. ``Before you decide that some of the policies that in fact go against our grain and our natural desire for openness, before you decide those are completely wrong and unacceptable, I hope you'll give a little thought to the people who go out there and defend us in secret and do so at great risk."



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Joe Abernathy <Joe.Abernathy@houston.chron.com> Wed, 24 Jun 92 18:10:02 CDT

The following is the written response to my request for an interview with the NSA. To the best of my knowledge, and according to their claims, it is the government's first complete answer to the many questions and allegations that have been made in regards to the matter of cryptography.

I would like to invite reaction from any qualified readers who care to address any of the issues raised herein. Please mail to edtjda@chron.com (713) 220-6845.

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE Serial: Q43-11-92 9

10 June 1992 Mr. Joe Abernathy Houston Chronicle P.O. Box 4260 Houston, TX 77210

Dear Mr. Abernathy:

Thank you for your inquiry of 3 June 1992 on the subject of cryptography. Attached please find answers to the questions that you provided our Agency. If any further assistance is needed, please feel free to contact me or Mr. Jerry Volker of my staff on (xxx) xxx-xxxx.

Sincerely,

MICHAEL S.CONN Chief, Information Policy

ENCL:

1. Has the NSA ever imposed or attempted to impose a weakness on any cryptographic code to see if it can thus be broken?

One of NSA's missions is to provide the means for protecting U.S. government and military communications and information systems related to national security. In fulfilling this mission we design cryptologic codes based on an exhaustive evaluation process to ensure to the maximum extent possible that information systems security products that we endorse are free from any weaknesses. Were we to intentionally impose weaknesses on cryptologic codes for use by the U.S. government, we would not be fulfilling our mission to provide the means to protect sensitive U.S. government and military communications and our professional integrity would be at risk.

2. Has the NSA ever imposed or attempted to impose a weakness on the DES or DSS?

Regarding the Data Encryption Standard (DES), we believe that the public record from the Senate Committee for Intelligence's investigation in 1978 into NSA's role in the development of the DES is responsive to your question. That committee report indicated that NSA did not tamper with the design of the algorithm in any way and that the security afforded by the DES was more than adequate for at least a 5-10 year time span for the unclassified data for which it was intended. In short, NSA did not impose or attempt to impose any weakness on the DES.

Regarding the draft Digital Signature Standard (DSS), NSA never imposed any weakness or attempted to impose any weakness on the DSS.

3. Is the NSA aware of any weaknesses in the DES or the DSS? The RSA?

We are unaware of any weaknesses in the DES or the DSS when properly implemented and used for the purposes for which they both are designed. We do not comment on nongovernment systems.

Regarding the alleged trapdoor in the DSS. We find the term trapdoor somewhat misleading since it implies that the messages sent by the DSS are encrypted and with access via a trapdoor one could somehow decrypt (read) the message without the sender's knowledge. The DSS does not encrypt any data. The real issue is whether the DSS is susceptible to someone forging a signature and therefore discrediting the entire system. We state categorically that the chances of anyone - including NSA - forging a signature with the DSS when it is properly used and implemented is infinitesimally small.

Furthermore, the alleged trapdoor vulnerability is true for ANY public key-based authentication system, including RSA. To imply somehow that this only

affects the DSS (a popular argument in the press) is totally misleading. The issue is one of implementation and how one goes about selecting prime numbers. We call your attention to a recent EUROCRYPT conference which had a panel discussion on the issue of trapdoors in the DSS. Included on the panel was one of the Bellcore researchers who initially raised the trapdoor allegation, and our understanding is that the panel -- including the person from Bellcore -concluded that the alleged trapdoor was not an issue for the DSS. Furthermore, the general consensus appeared to be that the trapdoor issue was trivial and had been overblown in the press. However, to try to respond to the trapdoor allegation, at NIST's request, we have designed a prime generation process which will ensure that one can avoid selection of the relatively few weak primes which could lead to weakness in using the DSS. Additionally, NIST intends to allow for larger modulus sizes up to 1024 which effectively negates the need to even use the prime generation process to avoid weak primes. An additional very important point that is often overlooked is that with the DSS the primes are PUBLIC and therefore can be subject to public examination. Not all public key systems provide for this same type of examination.

The integrity of any information security system requires attention to proper implementation. With the myriad of vulnerabilities possible given the differences among users, NSA has traditionally insisted on centralized trusted centers as a way to minimize risk to the system. While we have designed technical modifications to the DSS to meet NIST's requests for a more decentralized approach, we still would emphasize that portion of the Federal Register notice for the DSS which states: While it is the intent of this standard to specify general security requirements for generating digital signatures, conformance to this standard does not assure that a particular implementation is secure. The responsible authority in each agency or department shall assure that an overall implementation provides an acceptable level of security. NIST will be working with government users to ensure appropriate implementations.

Finally, we have read all the arguments purporting insecurities with the DSS, and we remain unconvinced of their validity. The DSS has been subjected to intense evaluation within NSA which led to its being endorsed by our Director of Information Systems Security for use in signing unclassified data processed in certain intelligence systems and even for signing classified data in selected systems. We believe that this approval speaks to the lack of any credible attack on the integrity provided by the DSS given proper use and implementation. Based on the technical and security requirements of the U.S. government for digital signatures, we believe the DSS is the best choice. In fact, the DSS is being used in a pilot project for the Defense Message System to assure the authenticity of electronic messages of vital command and control information. This initial demonstration includes participation from the Joint Chiefs of Staff, the military services, and Defense Agencies and is being done in cooperation with NIST.

4. Has the NSA ever taken advantage of any weaknesses in the DES or the DSS?

We are unaware of any weaknesses in the DSS or in the DES when properly implemented and used for the purposes for which they both are designed. 5. Did the NSA play a role in designing the DSS? Why, in the NSA's analysis, was it seen as desirable to create the DSS when the apparently more robust RSA already stood as a de facto standard?

Under the Computer Security Act of 1987, NIST is to draw upon computer systems technical security guidelines of NSA where appropriate and to coordinate closely with other agencies, including NSA, to assure:

a. maximum use of all existing and planned programs, materials, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

b. that standards developed by NIST are consistent and compatible with standards and procedures developed for the protection of classified systems.

Consistent with that law and based on a subsequent Memorandum of Understanding (MOU) between NSA and NIST, NSA's role is to be responsive to NIST's requests for assistance in developing, evaluating, or researching cryptographic algorithms and techniques. (See note at end). In 19??, NIST requested that NSA evaluate candidate algorithms proposed by NIST for a digital signature standard and that NSA provide new algorithms when existing algorithms did not meet U.S. government requirements. In the two-year process of developing a digital signature for U.S. government use, NIST and NSA examined various publicly-known algorithms and their variants, including RSA. A number of techniques were deemed to provide appropriate protection for Federal systems. The one selected by NIST as the draft Digital Signature Standard was determined to be the most suitable for reasons that were set forth in the Federal Register announcement. One such reason was to avoid issuance of a DSS that would result in users outside the government having to pay royalties. Even though the DSS is targeted for government use, eliminating potential barriers for commercial applications is useful to achieve economies of scale. Additionally, there are features of the DSS which make it more attractive for Federal systems that need to have a digital signature capability for large numbers of users. Chief among them are the number of trusted operation points and system management overhead that are minimized with the NIST proposed technique.

6. What national interests are served by limiting the power of cryptographic schemes used by the public?

We call your attention to the House Judiciary committee hearing of 29 April 1992. The Director of the FBI expressed his concerns that law enforcement interests in meeting responsibilities given to them by Congress could be affected unless they had access to communications, as was given to them by statute in 1968 (court monitored, court sponsored, court reviewed and subject to Congressional oversight).

The National Security Agency has no role in limiting the power of cryptographic schemes used by the public within the U.S. We have always been in favor of the use of information security technologies by U.S. businesses to protect their proprietary information, and when we had an information security role with private industry (prior to the Computer Security Act of 1987), we actively advocated use of such technologies. 7. What national interests are served by limiting the export of cryptographic technology?

Cryptographic technology is deemed vital to national security interests. This includes economic, military, and foreign policy interests.

We do not agree with the implications from the House Judiciary Committee hearing of 7 May 1992 and recent news articles that allege that U.S. export laws prevent U.S. firms' manufacture and use of top encryption equipment. We are unaware of any case where a U.S. firm has been prevented from manufacturing and using encryption equipment within this country or for use by the U.S. firm or its subsidiaries in locations outside the U.S. because of U.S. export restrictions. In fact, NSA has always supported the use of encryption by U.S. businesses operating domestically and overseas to protect sensitive information.

For export to foreign countries, NSA as a component of the Department of Defense (along with the Department of State and the Department of Commerce) reviews export licenses for information security technologies controlled by the Export Administration Regulations or the international Traffic in Arms Regulations. Similar export control systems are in effect in all the Coordinating Committee for Multilateral Export Controls (CoCom) countries as well as many non-CoCom countries as these technologies are universally considered as sensitive. Such technologies are not banned from export and are reviewed on a case-by-case basis. As part of the export review process, licenses may be required for these systems and are reviewed to determine the effect such export could have on national security interests - including economic, military, and political security interests. Export licenses are approved or denied based upon the type of equipment involved, the proposed end-use and the end-user.

Our analysis indicates that the U.S. leads the world in the manufacture and export of information security technologies. Of those cryptologic products referred to NSA by the Department of State for export licenses, we consistently approve over 90%. Export licenses for information security products under the jurisdiction of the Department of Commerce are processed and approved without referral to NSA or DoD. This includes products using such techniques as the DSS and RSA which provide authentication and access control to computers or networks. In fact, in the past NSA has played a major role in successfully advocating the relaxation of export controls on RSA and related technologies for authentication purposes. Such techniques are extremely valuable against the hacker problem and unauthorized use of resources.

8. What national interests are at risk, if any, if secure cryptography is widely available?

Secure cryptography widely available outside the United States clearly has an impact on national security interests including economic, military, and political.

Secure cryptography within the United States may impact law enforcement interests.

9. What does the NSA see as its legitimate interests in the area of cryptography? Public cryptography?

Clearly one of our interests is to protect U.S. government and military communications and information systems related to national security. As part of that mission, we stay abreast of activities in public cryptography.

10. How did NSA enter into negotiations with the Software Publishers Association regarding the export of products utilizing cryptographic techniques? How was this group chosen, and to what purpose? What statute or elected representative authorized the NSA to engage in the discussions?

The Software Publishers Association (SPA) went to the National Security Advisor to the President to seek help from the Administration to bring predictability, clarity, and speed to the process for exporting mass market software with encryption. The National Security Advisor directed NSA to work with the mass market software representatives on their request.

ii. What is the status of these negotiations?

These negotiations are ongoing.

12. What is the status of export controls on products using cryptographic techniques? How would you respond to those who point to the fact that the export of RSA from the U.S. is controlled, but that its import into the U.S. is not?

To the best of our knowledge, most countries who manufacture cryptographic products regulate the export of such products from their countries by procedures similar to those existing within the U.S. Some even control the import into their countries. The U.S. complies with the guidelines established by CoCom for these products.

Regarding the export of RSA from the U.S., we are unaware of any restrictions that have been placed on the export of RSA for authentication purposes.

13. What issues would you like to discuss that I have not addressed?

None.

14. What question or questions would you like to pose of your critics?

None.

NOTE: To clarify misunderstandings regarding this Memorandum of Understanding (MOU); this MOU does not provide NSA any veto power over NIST proposals. As was discussed publicly in 1989, the MOU provides that if there is an issue that can not be resolved between the two agencies, then such an issue may be referred to the President for resolution. Enclosed please find a copy of subject MOU which has been made freely available in the past by both NSA and NIST to all requestors. At the House Judiciary Committee hearings on 7 May 1992, the Director of NIST responded that he had never referred an issue to the White House since his assumption of Directorship in 1990.

#### MEMORANDUM OF UNDERSTANDING

#### BETWEEN

THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

AND

THE DIRECTOR OF THE NATIONAL SECURITY AGENCY

#### CONCERNING

THE IMPLEMENTATION OF PUBLIC LAW 100-235 Recognizing that:

A. Under Section 2 of the Computer Security Act of 1987 (Public Law 100-235), (the Act), the National Institute of Standards and Technology (NIST) has the responsibility within the Federal Government for:

1. Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security ad privacy of sensitive information in Federal computer systems as defined in the Act; and,

2. Drawing on the computer system technical security guidelines of the National Security Agency (NSA) in tis regard where appropriate.

B. Under Section 3 of the Act, the NIST is to coordinate closely with other agencies and offices, including the NSA, to assure:

1. Maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and, - 2. To the maximum extent feasible, that standards developed by the NIST under the Act are consistent and compatible with standards and procedures developed for the protection of classified information in Federal computer systems.

C. Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Computer System Security and Privacy Advisory Board, at least one of whom shall be from the NSA. Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:

The NIST will:

1. Appoint to the Computer Security and Privacy Advisory Board at least one representative nominated by the Director of the NSA.

2. Draw upon computer system technical security guidelines developed -by the NSA to the extent that the NIST determines that such guidelines are consistent with the requirements tor protecting sensitive information in Federal computer systems.

3. Recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation.

4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the ratest extent possible, in meeting these responsibilities in a timely and cost effective manner

5. Avoid duplication where possible in entering into mutually agreeable arrangements with NSA for NSA support.

6. Request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development valuation, or endorsement.

II. The NSA will:

1. Provide the NIST with technical guidelines in trusted technology, telecommunications security, and personal -identification that may be used in cost-effective systems for protecting sensitive computer data.

2. Conduct or initiate research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods.

3. Be responsive to the NIST's requests for assistance in respect to all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

4. Establish the standards and endorse products for application to secure systems covered in 10 USC Section 2315 (the Warner Amendment).

5 Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to Federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against that threat.

III. The NIST and the NSA shall:

1. Jointly review agency plans for the security and privacy of computer systems submitted to NIST and NSA pursuant to section 6(b) of the Act.

2. Exchange technical standards and guidelines as necessary to achieve the purposes of the Act.

3. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

4. Maintain an ongoing, open dialogue to ensure that each organization remains abreast of emerging technologies and issues effecting automated information system security in computer-based systems.

5. Establish a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified-information. The Group shall be composed of six Federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Deputy Director for Information Security or the NIST Deputy Director or may be generated -and addressed by the group upon approval by the NSA DDI or NIST Deputy Director. Within days of the referral of an issue to the Group by either the NSA Deputy Director for Information Security or the NIST Deputy Director, the Group will respond with a progress report and plan for further analysis, if any.

6. Exchange work plans on an annual basis on all research and development projects pertinent to protection of systems that process sensitive or other unclassified information, including trusted technology, technology for protecting the integrity and availability of data, telecommunications security and personal identification methods. Project updates will be exchanged quarterly, and project reviews will be provided by either party upon request of the other party.

7. Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical-systems security techniques to be developed for use in protecting sensitive information in Federal computer systems to ensure they are consistent with the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the NSC for resolution. No action shall be taken on such an issue until it is resolved.

8. Specify additional operational agreements in annexes to this MOU as they. are agreed to by NSA and NIST.

IV. Either party may elect to terminate this MOU upon six months written notice. This MOU is effective upon approval of both signatories.

RAYMOND G. KAMMER	W. O. STUDEMAN
Acting Director,	Vice Admiral U.S. Navy,
National Institute of	Director, National Security Agency
Standards and Technology	

[If any garbles remain, they are due either to the scanning process or to PGN trying to fix the originally very buggy scanned version. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 13: Issue 61



Jim Griffith <griffith@dweeb.fx.com> Wed, 1 Jul 92 23:10:30 PDT

Oakland station KTVU news reported that a Richmond refinery's emergency notification system was sabotaged by a disgruntled ex-employee, and the damage wasn't discovered until a leak caused the refinery officials to attempt to use it. Unfortunately, I didn't catch any names, but the gist of the story is that this refinery has a system in place which automatically dials nearby residents when accidents occur and informs them of emergency procedures that should be followed. Specifically, a recent leak caused them to activate the system in an attempt to warn residents to remain indoors for the duration. However, the system failed to operate. A subsequent investigation discovered that a former programmer who had been fired had sabotaged the system in revenge prior to leaving.

Authorities are reportedly planning on filing charges against the former employee once they figure out what charges are appropriate.

"Reckless endangerment" springs to mind. Hope they nail the guy to the wall.

Jim

[An item by Erin Hallissy in the San Francisco Chronicle, 2 July 1992, p.A19 had some details. The emergency alert network is run by the Community Alert Network. An EX-employee of their New York office (who has confessed to the malicious hacking) modified software ("reconfigured some things that caused it to crash") in their computer systems in both New York and San Jose. In this case, the incident occurred at the Chevron refinery. The network had been used four times previously (since last October) in Contra Costa County, twice for incidents at Chevron, once at Pacific Refinery in Hercules, and once for a fire at Rhone-Poulenc in Martinez. As a sidelight, the previously fired perpetrator broke into the NY office two days after the latest Chevron emergency, "maybe just to gloat". The system was down for 10 hours, during which time the only emergency was the one at Chevron. [Note that the system cannot call unlisted numbers or numbers listed without street addresses. PGN]

### Nutrasweet Telephone Sweepstakes

Ranjit Bhatnagar <ranjit@unagi.cis.upenn.edu> Sun, 28 Jun 92 17:56:59 EDT

Among the advertisements in this Sunday's (28 June) Philadelphia Inquirer, and probably most every other newspaper in the United States, was an announcement for the NutraSweet Summer Sweepstakes. It works as follows: call the free 800 number they provide, then punch in your phone number and the UPC code from any product containing NutraSweet, a sugar substitute. You are immediately told whether you won one of a few thousand prizes ranging from a tote bag to ten thousand dollars. In the fine print, it says that the sweepstakes will end after two million calls are received, or at a certain date in July, whichever comes first. It also says that the odds of winning depend on the number of calls received.

First point: the odds seems odd to me. Unlike a paper sweepstakes, where all the entries are received before the prizes are drawn, in this sweepstakes the winners are chosen immediately. The random selection process must have fixed odds built-in, probably based on a projection of exactly two million calls. Even if they have to cut off the contest before two million calls are received, the odds for a particular call would still be the same, and some fraction of the prizes would not be awarded.

Second point: the drawbacks of a sweepstakes where the entries are free data

calls are obvious. People with access to smart modems or autodialing machinery and the ability to program them have a significant advantage over those without. Many telephones nowadays have programmable dialers built in, but they're usually not as useful as the following command string for a Hayes-compatible modem:

ATDT 18002351000,,,,,,1,

### Kisk of Assuming an Int will do

"Russell Aminzade: Trinity College of VT" <AMINZADE@uvmvax.bitnet> Mon, 22 Jun 1992 12:08 EST

In the current (6/92) BYTE, Jerry Pournelle discusses his difficulties with using the word-count feature in Microsoft Word For Windows.

...when I would read in the file, Word For Windows told me there were 767,356 characters and 135,000 words; the word count was in gray, indicating that it was an estimate...clicking on [the 'update' button] caused the program to trundle for a while and then proudly announce a total of 60,273; which, of course was absurd...I've since learned, though, that all I needed to do was add 65,535 to the total shown...

Sounds like one of the wizards at Microsoft determined that an int rather than a longint was plenty big for the kind of documents people would be editing.

### Students cheated BT to win computerised phone contest

Philip Hazel <ph10@cus.cam.ac.uk> Wed, 1 Jul 92 11:06:36 BST

>From the "Cambridge Evening News", June 30 1992:

[HEADLINE] Students cheated BT to win phone contest

Two students swindled BT [British Telecom] out of 68,000 pounds [sterling] in a "lucrative scam" to constantly win on a telephone quiz game, a court heard. The two men hired four phone lines between them under false names and left the receivers off the hook for hours on end at a Cambridge flat to win thousands of pounds.

On one occasion, said a BT official outside court, a receiver was left off the hook for almost 24 hours. Eight or nine hours was the average, with peak rate calls at 48 pence a minute.

>From his winnings, Shaun Middleton bought an XR3i high-performance car and a computer, while his confederate, Tristan Abbott-Coates, also bought a computer. The pair were "determined to beat the system", Cambridge Crown Court heard, and hatched a scheme to constantly win on the "Wheel of Fortune" game advertised in the national press. The game has a 10,000 pound jackpot.

The pair rang the contest phone number, which was monitored by a computer. When the computer asked them questions, they made no response - and the computer was programmed to interpret silences as "no" answers.

The correct "no" answers accumulated into winning cash combinations.

A copy of the original advert, printed in The Sun newspaper, was presented as evidence. Judge Frederick Beezley asked if it was page three. [Page 3 of The Sun carries pin-up photographs.] When told it was not, he quipped, "Oh well, never mind, I'll suppose I'll look at it anyway."

Middleton, 22, of St George's Road, Preston, admitted three charges of obtaining services by deception. He won a total of 10,709 pounds but ran up an unpaid BT bill of 51,469 pounds. Abbott-Coates, 24, of the same address, admitted one charge of obtaining services by deception. He won a total of 2,672 pounds - but ran up an unpaid bill of 16,601 pounds.

The offences were committed while the two men each rented a room in Marshall Street, Cambridge, between March and September last year. They moved to Preston together to attend the polytechnic there.

Francis Sheridan, prosecuting, said that Abbott-Coates first recognised the loophole in the telephone quiz, but Middleton was the most active in the swindle. He said the pair used false names to hire the lines "to avoid being cut off and thus ending a lucrative scam". Abbott-Coates chose the alias Murphy after an actor who played a famous screen policeman.

Eventually, BT became suspicious and traced the pair to Preston. Both men were then arressted. Sentencing was adjourned until July 24 so that social enquiry reports could be made. Judge Beezley said he was considering a custodial sentence, and remanded both men in custody.

Internet: P.Hazel@ucs.cam.ac.ukUniversity Computing Service,JANET: P.Hazel@uk.ac.cam.ucsComputer Laboratory, Pembroke St,Phone: +44 223 334714Cambridge CB2 3QG, England.

# computer-literate children find porn

Andrew Shapiro <andrew@gooter.metronet.org> Fri, 26 Jun 92 12:05:26 MDT

Rocky Mountain News Mon., June 22,1992

COMPUTER-LITERATE CHILDREN FIND PORN AVAILABLE ON THEIR SCREENS AT HOME By James Michels, Scripps Howard News Service

Connie Lewis recently discovered one of the unpleasant shocks of patenting: pornographic pictures her 15-year-old son had collected.

What surprised her more was where she found them: on the screen of the family's home computer.

Her son had gotten them free from a local computer bulletin board.

### [..Deleted..]

The pornographic pictures could have been posted on the computer bulletin board by anyone. Lewis' son had learned about them from a friend.

The pictures were in an area of the board restricted to adults, but all the 15-tear-old had to do to get access was to type in false information about his name and age. He instantly gained access to dozens of pornographic pictures.

#### [..Deleted..]

The technology of putting pornographic pictures on computers and distributing them by telephone is so new it is unregulated.

Public officials say current laws don't appear to apply to the bulletin boards. Indiana Bell can block access to sexually explicit 900 numbers, but not to local numbers, such as those used by the boards.

The Federal Communication Commission, which regulates telephone lines, said the issue does not come under its jurisdiction.

The FBI is investigating a case in which a national computer board was used to pass along child pornography.

[..Deleted..]

So What's a responsible system operator to do?

He can threaten to close his board to those who misuse it, but that is often a hollow threat.

"You have a apparently strong warning that you can be banned and so on if you mislead the system operator," said Michael Banks, a Cincinnati computer writer familiar with bulletin boards

"The threat of being banned permanently is meaningless. If someone wants to get back on, they do it with a different name."

Even though this is a sensationalistic article designed to invoke a shock response in 'decent americans' (a risk in and of itself) there are several good points. If it is deemed a crime to distribute, electronically, pornographic images to minors then what sort of validation is enough? Who is actually responsible? Can the owner of the bulletin board be charged? Should the original poster be charged? In this day and age of store-and-forward worldwide networks how are legal boundaries handled? Is the system operator responsible for all the data stored on his machine?

-Andrew T. Shapiro, andrew@gooter.metronet.org

### VK ATMs - legal challenge

KPMG - Antony Upward,IVC <UPWARD.A@applelink.apple.com> 02 Jul 92 17:05 GMT

Banks face challenge over teller machines

Reproduced without permission from the Financial Times Weekend June 27/June 28 1992 edition.

Banks and building societies face their most serious legal challenge from customers over cash dispensing automated teller machines (ATMs), writes Barbara Ellis.

This is in spite of words of comfort from the Building Society Ombudsmen this week. They welcomed the new (pounds) 50 limit introduced by the Code of Banking Practice, on losses from unauthorised use of machines unless the bank can prove fraud or gross negligence.

Some 400 customers assembled into an action group by J. Keith Park, solicitors, of St Helens, Merseyside, are to seek a High Court ruling, within the next two to three weeks, that banks and building societies operating teller machines are in breach of contract beacuse the machines are suseptible to error and fraud.

Each of the 400 will make detailed claims for losses through alleged unauthorised withdrawals ranging from (pounds) 90 to (pounds) 13,000 and totalling close to (pounds) 500,000. All the claims have been rejected by banks and building societies.

For example, Barclays stated this week that out of its 15 million machine transactions each month, fewer than one in every 250,000 is disputed - which would imply 60 disputes a month. Dennis Whalley , of J.Keith Park, says he has deduced, from ATM dispute cases that disputes have been running close to 9,000 a month.

Barclays says there is no correlation between the volume of teller machine disputes and the reference numbers which relate to computer files. (Strange I haven't seen a computer program yet that didn't start counting at one with increments of one!)

For years banks and building societies have insisted that the ATM systems are completely secure and that money can only be withdrawn with the use of a card and personal identification number (PIN) [sic].

The obudsmen have almost inveriably backed the insitutions in rejecting claims from customers who detected "phantom" unauthorised withdrawals, saying that they must have unwittingly lost their cards, disclosed their PIN or been a victim of a dishonest family member.

However, the 1989 Jack report on banking acknowledged that the PIN system was open to fraud and last year an engineer employed by the Clydesdale Bank confessed to removing (pounds) 17,000 from customers' accounts by arranging phantom withdrawals using a hand-held computer.

# CPSR Challenges Virginia SSN Practice

<sobel@washofc.cpsr.org> Tue, 30 Jun 1992 19:45:42 -0400

PRESS RELEASE, June 30, 1992 CPSR Challenges Virginia SSN Practice

WASHINGTON, DC -- A national public interest organization has filed a "friend of the court" brief in the federal court of appeals, calling into question the Commonwealth of Virginia's practice of requiring citizens to provide their Social Security numbers in order to vote. Computer Professionals for Social Responsibility (CPSR) alleges that Virginia is violating constitutional rights and creating an unnecessary privacy risk.

The case arose when a Virginia resident refused to provide his Social Security number (SSN) to a county registrar and was denied the right to register to vote. Virginia is one of a handful of states that require voters to provide an SSN as a condition of registration. While most states that require the number impose some restrictions on its public dissemination, Virginia allows unrestricted public inspection of voter registration data -- including the SSN. Marc A. Greidinger, the plaintiff in the federal lawsuit, believes that the state's registration requirements violate his privacy and impose an unconstitutional burden on his exercise of the right to vote.

The CPSR brief, filed in the Fourth Circuit Court of Appeals in Richmond, supports the claims made by Mr. Greidinger. CPSR notes the long-standing concern of the computing community to design safe information systems, and the particular effort of Congress to control the misuse of the SSN. The organization cites federal statistics showing that the widespread use of SSNs has led to a proliferation of fraud by criminals using the numbers to gain driver's licenses, credit and federal benefits. The CPSR brief further describes current efforts in other countries to control the misuse of national identifiers, like the Social Security number.

Marc Rotenberg, the Director of the CPSR Washington Office said that "This is a privacy issue of constitutional dimension. The SSN requirement is not unlike the poll taxes that were struck down as unconstitutional in the 1960s. Instead of demanding the payment of money, Virginia is requiring citizens to relinquish their privacy rights before being allowed in the voting booth."

CPSR argues in its brief that the privacy risk created by Virginia's collection and disclosure of Social Security numbers is unnecessary. The

largest states in the nation, such as California, New York and Texas, do not require SSNs for voter registration. CPSR points out that California, with 14 million registered voters, does not need to use the SSN to administer its registration system, while Virginia, with less than 3 million voters, insists on its need to demand the number.

David Sobel, CPSR Legal Counsel, said "Federal courts have generally recognized that there is a substantial privacy interest involved when Social Security numbers are disclosed. We are optimistic that the court of appeals will require the state to develop a safer method of maintaining voting records."

CPSR has led a national campaign to control the misuse of the Social Security Number. Earlier this year the organization testified at a hearing in Congress on the use of the SSN as a National Identifier. CPSR urged lawmakers to respect the restriction on the SSN and to restrict its use in the private sector. The group also participated in a federal court challenge to the Internal Revenue Service's practice of displaying taxpayers' SSNs on mailing labels. CPSR is also undertaking a campaign to advise individuals not to disclose their Social Security numbers unless provided with the legal reason

#### for the request.

CPSR is a national membership organization, with 2,500 members, based in Palo Alto, CA. For membership information contact CPSR, P.O. Box 717, Palo Alto, CA 94303, (415) 322-3778, cpsr@csli. stanford.edu.

For more information contact:

Marc Rotenberg, Director or David Sobel, Legal Counsel CPSR Washington Office, (202) 544-9240 rotenberg@washofc.cpsr.org or sobel@washofc.cpsr.org

Paul Wolfson, attorney for Marc A. Greidinger Public Citizen Litigation Group (202) 833-3000

# Are Humans Always Responsible for Computer Errors? (Davis, <u>RISKS-13.54</u>)

Peter Danielson <danielsn@unixg.ubc.ca> Wed, 24 Jun 92 11:30:08 PDT

While I concur with Davis' criticism of the anthromorphic attribution of the mistake to the Endeavour's computer, I cannot accept the assumptions about responsibility that seem to stand behind this criticism.

He seems to assume that whenever something goes wrong, some human did wrong. This is clearly too strong. Most technological causation works through groups (teams, firms). But even the weaker assumption that all wrong is attributable to humans -- let me call it Complete Human Responsibility, or CHR -- is problematic.

My point is that CHR is not obviously true. It is trivial to note that some bad events \*just happen\*. I do not see why this is not the case with artifacts as well. People are not naturally responsible for everything that happens, just because people made the object(s) involved. I suggest that we see CHR as a value or standard, not a report of a fact about the world. But then CHR needs to be argued for.

The risk? Taking a (controversial) matter of principle to be a simple fact.

Peter Danielson, Centre for Applied Ethics, University of British Columbia

# Fokker F.100 incident

Robert Dorsett <rdd@rascal.ics.utexas.edu> Tue, 23 Jun 92 23:15:12 CDT

An interesting little story from AIRLINE PILOT, May 1992 issue ("No Brakes, No Reversers!", by Joseph J. Poset, USAir).

It deals with a Fokker F.100 which landed at Chicago O'Hare, on November 21, 1991, with thrust reversers and brakes inoperative. The F.100 is a

higher-capacity, fundamentally redesigned version of the Dutch company's popular F.28. It is a twin-engine, T-tailed "commuter" jet, in the 100-120 seat capacity. It was certified in November 1987. It has a "glass cockpit," but is \*not\* an FBW airplane, at least as far as flight control is concerned.

Essentially: the flight landed on Chicago's Runway 22L. Upon landing, the crew discovered their brakes and thrust reversers weren't working. They took the high-speed turnoff (a taxiway oriented about 30 degrees off the runway), shut down one engine, zipped down the parallel taxiway, turned left at the end of it (90-degree U-turn), went back up Runway 4R (reciprocal runway of the one they landed on), took the \*opposite\* high-speed taxiway, and headed onto Runway 27, which an American Airlines jet had just taken off from. Twice, the captain thought he would have had to turn off the pavement into the rough, to avoid a collision.

After they finally came to a stop on Runway 27, the crew noticed that their flight computers thought they were still in the air. The stickshaker (stall warning) was also activated, and the "speed limit" flag on their flight display (indicating excursion outside the approved flight envelope) was on.

After some investigation, it was discovered that both Air/Ground switches (located on the landing gear) were each "stuck," thus relaying improper data to the computers and devices which controlled the stickshaker, various annunciators, reversers, and ground braking. It was only after maintenance applied glycol that the computers indicated the proper modes.

Now, there's nothing new about the use of Air/Ground switches--they're used, for instance, to prevent the inadvertent application of reverse thrust in flight, for most airliners. They're also used to deactivate stall-warning systems on the ground. But this is a pretty widespread set of high-level services that were affected by the switches being out of whack. I don't believe, for instance, that the A/G switch is used to establish whether wheel braking is available, on most airliners. It also has interesting ramifications to FBW aircraft, which might use an independent "ground control" mode to determine how everything from nosewheel steering to rudder control to wheel brakes work. In this case, if the airplane did not have nosewheel steering (for instance, if the design was highly compartmentalized into "ground" services and "air" services), it may have gone off the high-speed taxiway, into the rough, and ended up on yet another runway. This could have been a major accident...

There is a "flight-test" article on the F.100 in the January 30, 1998, issue of FLIGHT INTERNATIONAL, by Harry Hopkins ("Fokker 100: protect by wire."). It's interesting reading.

Robert Dorsett, Internet: rdd@rascal.ics.utexas.edu UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

### Ke: Fokker F.100

Robert Dorsett <rdd@rascal.ics.utexas.edu> Wed, 24 Jun 92 15:50:21 CDT More info on the Fokker incident. Note that it wasn't based on an ASRS report; I had confused it with another article. R.

>I hate to say it, but I find that incident pretty unbelieveable.>Firstly, I can't imagine that, if the Fokker had enough momentum to>need to come back on runway 4, that it wouldn't have groundlooped>around the 180 (90?) degree turn.

The article said they had a 25G38 kt headwind on roll-out. Around 40-50 kt at the first high-speed exit. But then again, if they hadn't stopped by the loop back up RWY 4, that headwind would have become a TAILWIND... The article indicates they started \*accelerating\* up RWY 4. They entered the other high-speed exit at 20-30 knots.

>Also, F100's like F28's, don't

>\*have\* thrust reversers, so the continual reference to them worries me.

It was penned by the captain, based upon his ASRS report. He was much more inexperienced than his F/O, but surely not that much! :-)

>Are you sure of the veracity of the publication?

Absolutely not. It's garbage. But the occasional article catches my interest.

>It wasn't dated April 1 or something?

No. I went to the FLIGHT article cited, looking for more information. Generally, it played up Fokker's in-flight protections; it's quite interesting. Little on systems.

On the last page: "Final roll-out to a standstill was made without reverse thrust, and with late minimum braking for test purposes. Rudder and pedal steering completed a halt within 2ft of the centerline. Reverse was restricted temporarily to idle anyway, because full reverse efflux can impinge on the tailplane, and a modification will set a gap between the two target doors to spill some flow centrally. The F.28 is not fitted with reversers.

"Reverse opeation is shown by a green 'R' at the top of the primary engine instrument display, but I did not find it compelling. A brighter panel, nearer to peripheral vision, would be easier to take in."

Perhaps reversers were INOP on early models, or are optional equipment. I don't imagine there's a compelling need for them on the lighter configurations, but this is probably a regulatory issue.

Robert

# 🗡 Another Fokker F.100 incident

Olivier PLAUT <plaut@sc2a.unige.ch> 29 Jun 92 12:29:04 +0200 A Swissair pilot reported to me another incident he had with a F100 just a few days ago: they had no flaps for landing.

The computer controls if flaps on both wings are extending together, and if not, it blocks to avoid an asymetrical configuration.

The flaps were moving correctly, but the computer had a false indication and did not permit to extend them.

The aircraft landed without problem at 160 KTS instead of 130. The passengers didn't even remark an abnormality.

Olivier Plaut, Institute of Forensic Medicine, Toxicology Unit, University of Geneva, Av. de Champel 9, CH-1211 Geneve 4, Switzerland +41 (22) 702.56.12



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# Mewsweek Vincennes article

<Bob\_Frankston@frankston.com> Wed 8 Jul 1992 14:02 -0400

I'd be interested in comments on its accuracy.

I won't comment on the larger issues of the "if it moves, shoot it" mentality. But as a systems designer I can understand the compromises made to meet the specs, but two small points stick in my mind.

One is the image of a technician madly scanning through a dog-eared issue of the OAG (the article didn't mention a brand name) to find the Iranian flight. It's hard enough to not miss an entry when in a quiet airport in a single time zone. I realize that tracking civilian flights was not part of the normal battle plan, but I presume that the system has still not been updated to link to the civilian airline reservation systems or other such sources of information. One change in warfare, which I think the Gulf War illustrated, is how the commercial technology has, in many ways, surpassed the military. Of course, the online airline info might not be accurate which means a delayed flight could still have been missed.

The other is that the tagging of the plane as an F-14 provided for no level of ambiguity. Even in the heat of battle, can the system cope with multiple interpretations of data or does it mindless lock in on a worst case and then present it to the befuddled user as fact?

Of course, dealing with ambiguous information from many sources is a very difficult problem and, as this incident illustrates, neither the system nor the users are up to task. Conversely, what good is SDI if the incoming missiles all follow commercial airline schedules?

[The article was based on a new report produced jointly by Newsweek and the ABC "Nightline" (and scheduled to be broadcast on ABC on 1 July). The report challenges the official U.S. account, claiming that U.S. forces had "provoked the episode". It also cites Admiral Crowe as confirming that the Vincennes was in Iranian waters at the time. The Pentagon replied that that was true, but only in self-defense. Source: NYTimes, 2 July 1992.

For those of you who don't remember the technological aspects of the Aegis system, see my item recounting a discussion with Matt Jaffe in <u>RISKS-8.74</u> (and a follow-on in 8.75). For anyone seriously interested in this bit of technohistory, I recommend your rereading the lead item in <u>RISKS-8.74</u>. PGN]

# Are bank machines private?

Andre Bacard <abacard@well.sf.ca.us> Wed, 8 Jul 92 15:01:04 -0700

[I just returned from Paris, where I read the following article in the "European" newspaper. Hmm...]

PIN Money for Thieves"

Italian thieves have managed to pull off the world's most ingenious cash card fraud. A perfect replica of a bank cash dispenser was glued on top of the real thing and swallowed cards inserted by unsuspecting customers when they tried to withdraw money.

Police say that the thieves collected 104 cards before staff at the bank, in Busto Arsizio, near Milan, were alerted.

Normally a stolen bank card is useless without the owner's Personal Identification Number. But the thieves programmed their fake machine to request the customers' PIN numbers before telling them the card had been accidentally demagnetized and was being retained. After collecting the cards, the thieves then spent the night withdrawing money from genuine cash dispensers.

A police spokesman said: "The thieves have been having a spree, withdrawing money with the credit cards and the right PIN numbers. They were obviously electronics experts."

Andre Bacard, POBox 3009, Stanford, California 94309-3009 abacard@well.sf.ca.us (e-mail) (415) 897-6067 (voice)

[Another variant on the old spoofing attack. PGN]

# Virus consumes clerks at Sears

Kurt Guntheroth <kurt@tc.fluke.com> Tue, 7 Jul 92 14:49:57 PDT

My mother-in-law is a sales clerk at a Sears store in Everett Washington. I saw 25 new CompuAdd point-of-sale terminals in the back room. They're super techie, with a small CRT, ASCII keyboard, fancy strip printer, and mag card stripe reader. They were supposed to be installed months ago, but apparently they have a dose of the Michaelangelo virus.

"Michaelangelo? On a terminal? Are you sure?" I asked. Needless to say, the answer was not too specific. She said it might also have been on a PC that configures the terminals, rather than the terminals themselves. Doesn't Michaelangelo only strike on one day of the year? All she knew was that they were "full of viruses" and could not be installed.

Sears has its share of troubles these days, and apparently it is running so lean and mean that there is no one in the store with enough computer smarts to get things cleared up in the intervening months. So there they sit, depreciating. But they'll \*sell\* you a computer...If you dare...bwah ha ha!

And you thought people who knew what viruses are were scared...

# ✓ GI Observations on IT Security Evaluation Manual (ITSEM) V0.2

Kai Rannenberg <kara@cs.tu-berlin.de> Tue, 7 Jul 1992 21:30:44 +0200

The Data Protection & Data Security Task Force of the German Gesellschaft fuer Informatik (GI) has again published a "Statement of Observations" concerning the IT Security Evaluation initiative driven by the Commission of the European Communities.

This time the statement had to be made on the Information Technology Security Evaluation Manual (ITSEM) in its current Version 0.2. The ITSEM shall give help to evaluators and sponsors working with Information Technology Security Evaluation Criteria (ITSEC) and therefore are related quite closely to them. The current version 1.2 of ITSEC was subject of the last "Statement of Observations" the GI Task Force published in February 1992. Discussion of Criticism on ITSEM shall take place in Brussels (Belgium) from September 8th to September 10th 1992.

Observations, criticism and proposals on ITSEM V0.2 concentrate on the following issues:

- (1) Lack of Correction of ITSEC problems
- (2) ITSEC needs much deeper and therefore more improvements than admitted in chapter 1.5.
- (3) Who oversees the Certification Bodies?
- (4) Several Classes of potential attackers are not covered.
- (5) Threats can not be enumerated and must be specified the other way round.
- (6) The discrimination between strength of mechanisms in only 3 classes (basic, medium or high) is very poor and not adequate.
- (7) Requirements for Tools and Techniques are missing.

The full statement is posted to alt.security, comp.security.misc and probably comp.society.privacy.

Kai Rannenberg, Technische Universitaet Berlin, Informatics, FR 5-10, Franklinstr. 28/29, D-W-1000 Berlin 10, Germany (+49 30) 314-73499

# 🗡 Voting by Phone in Nova Scotia

Evan Ravitz <evanr@alumni.cs.colorado.edu> Tue, 7 Jul 92 23:27:36 -0600

WORLD'S FIRST VOTING BY PHONE: JUNE 20 IN NOVA SCOTIA

After an initial failure on June 6, the Liberal Party of Nova Scotia held a primary June 20 to elect its next leader: 94% of the 7416 delegates voted, all with touch-tone phones. Typical turnout for Canadian elections is 60-70%.

The Liberals were issued Personal Identification Numbers by mail. For each of 2 ballots, voters called one of five 900 numbers corresponding to their choice of leader, and then keyed in their "PIN number". The computer then checked their number off so they couldn't vote again. John Savage won on the second ballot with almost 53% of the vote.

The service was provided by Maritime Telephone & Telegraph and cost each voter 50 cents. The eight-digit PIN numbers enabled one to vote from any billable touch-tone phone: if you did't have touch- tone, you'd borrow your neighbor's. Absentee voting was as simple as picking up the phone, wherever you were.

With this success, the Canadian government is considering a national referendum by phone on the results of their Constitutional Convention, within 6 months.

The Federal Voter Assistance Program of the Pentagon is now considering voting by phone for servicemen, who had voting by fax from the Persian Gulf. But a \$300 fax machine is overkill when a \$10 touch-tone phone will do. The Program called the Voting by Phone Foundation of Boulder for their initial information.

The Voting by Phone Foundation is now in a petition drive to put a charter amendment on November's Boulder City ballot. If passed Boulder would become the first city in the U.S. to offer the option of phone voting. Please call [Evan at] (303)444-3596 to help.

The Foundation is holding a demonstration of voting by phone from now until the November 3rd election. Anyone may call (303)444-3596, 24 hours a day. If you are registered to vote in Boulder, you will be asked to enter your last name and birth date for identification. This limits you to one vote, although not as effectively as the random PIN number to be used for real elections. A different question will be asked every 2 weeks, and presidential [... rest truncated by Evan's mailer?]

### When Cryptography is Outlawed...

Kurt Guntheroth <kurt@tc.fluke.com> Tue, 7 Jul 92 09:03:29 PDT

When Cryptography is Outlawed, Only Outlaws Will Have Cryptography

The really difficult-to-understand part about the Federal Government's recent assault on cryptographic privacy is how the Feds think they'll keep cryptography out of the hands of criminals and Evil Foreign Governments.

Now that the Feds have admitted that they have trouble decoding encrypted messages, any criminal or Evil Spy with a brain will be rushing to purchase the equipment. Criminals are hardly worried about breaking any law that says they can't keep their deeds a secret, and smuggling the technology into the country will hardly pose a problem to a reasonably proficient Drug Lord.

Perhaps what the Feds are looking for is a new weapon of prosecution; use of cryptography is by definition a felony, and widespread use of cryptography is then by definition racketeering as defined by RICO. It's like bagging Capone for tax evasion, when he was too slippery to be caught breaking the law. I find this sloppiness unacceptable as a taxpayer.

It's just like illegal weapons. The crooks have the Uzis and MAC-10s, and the cops have .38s. And the streets are nevertheless protected. I see a future where the world class criminals profit from breaking our insecure-bylegal-decree comm systems, preying on us law abiding citizens, while carrying out their business in unlawful security.

Why can't the spies get wise? Technology is not static. If the phone becomes secure, there must be improvements in bugging or some other spook-versus-crook technology that could replace this information gathering avenue.

How typical of our freedom-loving government to make keeping a secret felonious.

[By the way, see the July issue of the CACM, which contains material some of

which has appeared earlier in RISKS, plus a piece by John Perry Barlow and a a response to letters from Rivest, Hellman, and Anderson from John Lyons of NIST. PGN]

### Ke: computer-literate children find porn (<u>RISKS-13.62</u>)

Karl Lehenbauer <karl@sugar.neosoft.com> Sun, 5 Jul 92 11:10:05 CDT

That same 15-year-old can see some pretty steamy R-rated movies on his family's cable TV movie channels, or over at his friends. He can trade videotapes. Many mainstream magazines, such as Vogue, purchasable over the counter by anyone, contain photographs of partially nude women.

It would be tragic if heavy legal restrictions placed on "computer porn", when it is so difficult to police users' actions and impossible to monitor all activity on any moderately large BBS in any case, and when "pornography" is so readily available to everyone through so many other channels, for many of which no attempt is made to validate the recipient's age at all.

With the ongoing fusion of communications technologies such as computers, telephones and television, the restrictions' boundaries would broaden to encompass more and more of the technologies available to us to communicate with. Further, since the technology for copying and forwarding images (video, PC, etc) is so pervasive, enforcement would be spotty and selective, with many innocent people, for example those whose systems were unknowingly used to further these peoples' purposes, caught in the net.

# ✓ ESORICS 92: Preliminary Programme

Yves Deswarte <deswarte@laas.laas.fr> Tue, 7 Jul 92 10:08:07 +0200

Please find enclosed the preliminary ESORICS 92 programme in its ASCII English version. PostScript versions of the full programme can be accessed by ftp at "laas.laas.fr" (140.93.0.15), in files : ~ftp/pub/esorics/PGM.PS : PostScript file without laserprep ~ftp/pub/esorics/PGM.PS.Z : idem in compressed form (binary) ~ftp/pub/esorics/PGM.PS.long : PostScript file with laserprep ~ftp/pub/esorics/PGM.PS.long Z : idem in compressed form (binary)

If you wish to receive a paper copy, drop me mail. Yves

===== Yves Deswarte - LAAS-CNRS & INRIA - 31077 Toulouse (France) ===== ==== E-mail:deswarte@laas.fr - Tel:+33/61336288 - Fax:+33/61336411 ====

ESORICS 92 Preliminary Programme European Symposium on Research in Computer Security November 23-25, 1992, Toulouse, France Computer security is concerned with the protection of information in environments where there is a possibility of intrusion or malicious action. The aim of ESORICS 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 under the best conditions, ESORICS 92 will be a single track symposium and the selected papers will be presented in a conference hall whose capacity is 290 attendees. ESORICS 92 is the second symposium of a series started with ESORICS 90 held in Toulouse in October, 1990.

Symposium Chair: Gerard Eizenberg (ONERA/CERT, France)

#### Organized by AFCET

#### In Cooperation with

- BCS The British Computer Society
- CNRS Centre National de la Recherche Scientifique
- DISSI Delegation Interministerielle pour la Securite des Systemes d'Information
- DRET Direction des Recherches Etudes et Techniques
- ERCIM European Research Consortium for Informatics and Mathematics
- GI Gesellschaft fur Informatik
- IEE Institute of Electrical Engineers
- INRIA Institut National de Recherche en Informatique et Automatique
- NGI Nederlands Genootschap voor Informatica

#### PROGRAMME

#### Monday, November 23, 1992

9:00-10:30 Registration and welcome coffee
10:30-11:00 Introduction to ESORICS 92
11:00-12:30 Session: Access Control
Towards security in an open systems federation
(John A. Bull, Li Gong, Karen R. Sollins)
Type-level access controls for distributed structurally object-oriented
database systems (Udo Kelter)
On the Chinese wall model (Volker Kessler)
12:30-14:15 Lunch
14:15-15:45 Session: Formal Methods
Formal methods and automated tool for timing-channel identification in TCB
source code (Jingsha He, Virgil D. Gligor)
Separating the specification and implementation phases in cryptography
(Marie-Jeanne Toussaint)
Formal specification of security requirements using the theory of
normative positions (Andrew J. I. Jones, Marek Sergot)
15:45-16:15 Break
16:15-17:45 Invited Talks
Roger Needham: Key management (to be confirmed)
Yvo Desmedt: Different views on security
18:00 Buffet
18:30 Poster Session

[ESORICS 92 will include Poster Sessions devoted to presentations on work in progress, recent research results and innovative proposals. These poster sessions will be held in rooms with paperboards and poster supports, these rooms being available at any time from the beginning to the end of the symposium. If you are interested in posting a presentation, please submit a short description of your presentation with your registration before September 30, 1992. Notification of acceptance or rejection will be sent by October 25, 1992].

#### PROGRAMME

Tuesday, November 24, 1992

8:30-9:00 Welcome coffee

9:00-10:30 Session: Authentication I Verification and modelling of authentication protocols (Ralf C. Hauser, E. Stewart Lee) KryptoKnight authentication and key distribution system (Refik Molva, Gene Tsudik, Els Van Herreweghen, Stefano Zatti) Associating metrics to certification paths (Anas Tarah, Christian Huitema) 11:00-12:30 Session: Distributed Systems An object-oriented view of fragmented data processing for fault and intrusion tolerance in distributed systems (Jean-Charles Fabre, Brian Randell) The development and testing of the identity-based conference key distribution system for the RHODOS distributed system (M. Wang, A. Goscinski) Policy enforcement in stub autonomous domains (Gene Tsudik) 14:15-15:45 Session: Authentication II Freshness assurance of authentication protocols (Kwok-Yan Lam, Dieter Gollmann) A formal framework for authentication (Colin Boyd) Timely authentication in distributed systems (Kwok-Yan Lam, Thomas Beth) 16:15-17:00 Invited Talk Yvon Klein: What research for security evaluation ? 17:00-18:15 Panel: Availability and Integrity 18:30-... Poster Session 20:00-... Banquet PROGRAMME Wednesday, November 25, 1992 8:30-9:00 Welcome coffee 9:00-10:30 Session: Database Security Polyinstantiation for cover stories (Ravi S. Sandhu, Sushil Jajodia) On transaction processing for multilevel secure replicated databases (I. E. Kang, T. F. Keefe) Security constraint processing in multilevel secure AMAC schemata (G. Pernul) 11:00-12:00 Session: System Architectures M2S: A machine for multilevel security (Bruno d'Ausbourg, Jean-Henri Llareus) GDoM, a multilevel document manager (Christel Calas)

13:45-15:15 Session: Applications UEPS - A second generation electronic wallet (Ross J. Anderson) A hardware design model for cryptographic algorithms (Joan Daemen, Rene Govaerts, Joos Vandewalle) ASAX: Software architecture and rule-based language for universal audit trail analysis (Naji Habra, B. Le Charlier, A. Mounji, I. Mathieu) 15:15-15:30 Closing Remarks Programme Committee: Jean-Jacques Quisquater (UCL, Belgium), Chair Bruno d'Ausbourg (ONERA-CERT, France) Joachim Biskup (Universitat Hildesheim, Germany) Peter Bottomley (RSRE, United Kingdom) Yvo Desmedt (University of Wisconsin-Milwaukee, USA) Yves Deswarte (LAAS-CNRS & INRIA, France) Gerard Eizenberg (ONERA-CERT, France) Amos Fiat (University of Tel-Aviv, Israel) Dieter Gollmann (University of London, United Kingdom) Franz-Peter Heider (GEI, Germany) Jeremy Jacob (Oxford University, United Kingdom) Helmut Kurth (IABG, Germany) Jean-Claude Laprie (LAAS-CNRS, France) Peter Landrock (Aarhus University, Denmark) Teresa Lunt (SRI, USA) John McDermid (University of York, United Kingdom) John McLean (NRL, USA) Catherine Meadows (NRL, USA) Jonathan Millen (MITRE, USA) Emilio Montolivo (Fondazione Ugo Bordoni, Italy) Roger Needham (University of Cambridge, United Kingdom) Alfredo de Santis (Universita di Salerno, Italy) Einar Snekkenes (NDRE, Norway) Marie-Jeanne Toussaint (Universite de Liege, Belgium) Kioumars Yazdanian (ONERA-CERT, France)

Organization Committee:

Yves Deswarte (LAAS-CNRS & INRIA, France), Chair Laurent Cabirol (SCSSI, France) Jean-Francois Cornet (Consultant, France) Michel Dupuy (ENST, France) Marie-Therese Ippolito (LAAS-CNRS, France) Marie-France Kalogera (AFCET, France) Paul Richy (CNET, France) Pierre Rolin (ENSTA, France) Kioumars Yazdanian (ONERA-CERT, France)

#### **GENERAL INFORMATION**

Symposium Location: Hotel Palladia 271 avenue de Grande Bretagne, 31300 Toulouse, France telephone: +33 62 120 120, fax: +33 62 120 121 Hotel Palladia is located in the west district of Toulouse, 5 km from city centre. Access to Toulouse:

- By plane: Toulouse-Blagnac International Airport (telephone: +33 61 42 44 00). Hotel Palladia is 4 km from the airport. Approximate taxi fare is 50 FF.
- By train: Toulouse-Matabiau railway station (telephone:
  +33 61 62 50 50). Bus 14 from railway station to "Chardonnet" stop (in front of Hotel Palladia). Approximate taxi fare is 70FF.
- By car: Toulouse is linked to the main European road networks. On the Toulouse ring, direction Auch, exit 1 to Casselardit-Purpan.

Tourist Information: Office du Tourisme, Donjon du Capitole, 31000 Toulouse, telephone: +33 61 11 02 22

Visa: For non European Community citizens, please check with the French Consulate in your home country if you need a visa. Visa applications take approximately 4 weeks to process.

**Registration Procedure:** 

- Advance: Please complete the registration form and send it to AFCET. About 15 days before the beginning of the symposium, registered participants will receive their pass, which is to be presented at the registration desk to receive symposium documents.
- On-Site: Registration desk and welcome service will be available from 8:30 am to 8:00 pm on Monday 23, to 7:30 pm on Tuesday 24 and to 4:00 pm on Wednesday 25.
- Fellowships: Applications for half-rate registrations can be sent to AFCET with due justification. Students wishing to apply for these fellowships should join a recommendation letter from their professor.
- Fees: Registrations fees include admission to the technical sessions, one copy of the proceedings, breaks, lunches, Monday buffet and Tuesday banquet.

Payments: Payments are accepted in French Francs only:

- by credit cards (Visa International or MasterCard only): complete the charge authorization on the registration form.
- by banker's draft (with indication of your name and ESORICS 92), to the order of AFCET, bank account 502 650 009-02 at BIMP, 22 rue Pasquier, 75008 Paris, France. Please ask your bank to arrange the transfer at no cost for the beneficiary. Bank charges, if any, are at the participant's expense. To guarantee your registration, enclose a copy of your bank transfer.
- Cancellations: Refunds of 50% will be made if a written request is received before October 23, 1992. No refunds will be made for cancellations received after this date. In case of symposium cancellation for reasons beyond its control, AFCET limits its liability to the registration fees already paid.
- Proceedings: ESORICS 92 proceedings will be distributed on-site to registered participants. Extra copies of ESORICS 92 and ESORICS 90 proceedings will be sold on-site.

Languages: English and French, with simultaneous translation.

Social Event: A dinner banquet will be offered to all registered participants on Tuesday, November 24, 1992. For accompanying persons, banquet price is 250 FF.

Post-Symposium Tour: A visit (by bus) of Toulouse, the medieval city of Carcassonne and their region will be organized on Thursday, November 26, 1992. If interested, please tick the corresponding box on the registration form to receive tour information.

Travel Discounts: About 35% reduction for some Air Inter domestic return flights can be obtained for the Symposium dates. Please tick the appropriate box on the registration form to receive your discount voucher.

Hotel Reservations: There are many hotels in Toulouse in every category. A list of hotels, within walking distance from Hotel Palladia and offering special prices to ESORICS 92 participants, is given at the end of this message. For your reservation, please contact DIRECTLY the hotel of your choice; do not forget to mention ESORICS 92.

Local Organization: Marie-Therese Ippolito, LAAS-CNRS, 7 avenue du Colonel Roche, 31077 Toulouse (France), telephone: +33 61 33 62 74, fax: +33 61 55 35 77, E-mail: esorics@laas.fr.

#### **REGISTRATION FORM**

To be sent to: AFCET - ESORICS 92 156, boulevard Pereire 75017 Paris (France) Fax : +33 1 42 67 93 12 Telephone: +33 1 47 66 24 19

(Please print)

Name: First Name: Company: Address:

Country: Telephone : Fax : Nb of invoices requested: Invoice(s) to be sent to:

Air Inter Discount
[] Please send me an Air Inter discount voucher

Post-Symposium Tour
[] Please send me tour information

Poster Session
[] I wish to present a poster and I enclose its description.

FEE (18.6% VAT included):

Member: AFCET [] BCS [] GI [] IEE [] NGI [] Before October 24, 1992 : 3000 FF [] After October 23, 1992 : 3500 FF []

Non member: Before October 24, 1992 : 3300 FF [] After October 23, 1992 : 3800 FF []

Accompanying persons for banquet: x 250 FF

TOTAL : FF

PAYMENT (enclosed):

Banker's draft [] Purchase order [] Credit Card Authorization: I duly authorize you to charge my Visa Intl [] MasterCard [] Expiration : Card Number: Card holder name: Signature: Date :

#### HOTEL LIST

For all reservations, contact DIRECTLY the hotel of your choice, mentioning ESORICS 92, and confirm your reservation by fax or telex.

Palladia \*\*\*\* 271 avenue de Grande Bretagne, 31300 Toulouse telephone : +33 62 120 120 fax : +33 62 120 121 single 490 FF, breakfast 70 FF (Free shuttle available on request from the airport)

Dotel \*\*\* Avenue des Arenes Romaines, 31300 Toulouse telephone : +33 61 83 83 fax : +33 61 31 00 10 single 320 FF, breakfast included (Free shuttle available on request from the airport)

Novotel Toulouse Purpan \*\*\* 23 Impasse Maubec, 31300 Toulouse telephone : +33 61 49 34 10 fax : +33 61 49 63 37 single 430 FF, breakfast 47 FF (Free shuttle available on request from the airport)

Le Grande Bretagne \*\*\* 300 avenue de Grande Bretagne, 31300 Toulouse telephone : +33 61 31 84 85 fax : +33 61 31 87 12 single 390 FF, breakfast included

Campanile Purpan \*\* 33 route de Bayonne, 31300 Toulouse telephone : +33 61 31 09 09 fax : +33 61 31 09 10 single 240 FF, breakfast 29 FF

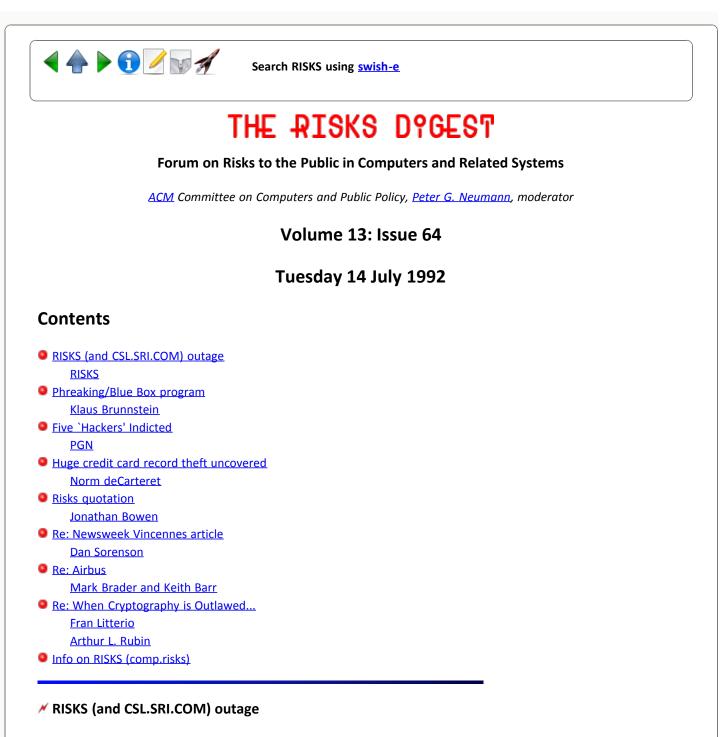
Gascogne \*\* 25 allees Charles de Fitte, 31300 Toulouse telephone : +33 61 59 27 44 telex : 521090F single 230 FF, breakfast 35 FF (3 km from Hotel Palladia, bus 14 "Saint-Cyprien" stop)

===== Yves Deswarte - LAAS-CNRS & INRIA - 31077 Toulouse (France) ===== ==== E-mail:deswarte@laas.fr - Tel:+33/61336288 - Fax:+33/61336411 ====



Search RISKS using swish-e

Report problems with the web pages to the maintainer



RISKS Forum <risks@csl.sri.com> Tue, 14 Jul 92 17:19:10 PDT

Due to a major disk crisis early Saturday from which RISKS has just recovered, some mail to CSL.SRI.COM may have been rejected. Please resubmit NOW if that was the case with anything you sent to RISKS or RISKS-REQUEST. When I finally was able to check my mail, a big gap on send dates is evident. Thanks. PGN

# Phreaking/Blue Box program

<br/><br/>brunnstein@rz.informatik.uni-hamburg.dbp.de>

#### Mon, 6 Jul 1992 21:42:49 +0200

CAPITAL, a German monthly specialized in financial aspects of economy, had a story, in it's July edition, about a phone phreak "Kimble" who offers an AMIGA-based program with built-in frequencies to switch your telecom connection over more than 20 countries. In June, he demonstrated this program in CAPITAL's office in Duesseldorf, in the presence of some experts from a criminal agency and an IT security experts. German Telecom was informed days ahead the presentation but could not trace his dialling experiments which lead him from Duesseldorf to Canada (known as normal entry of European Phreaks to the New World), and so on. Kimble said that non-traceability be a major new feature of this blue-boy program "Unlimited Assess (Multi-Frequency Dialler)".

Phreaking was practiced, for some time, also in Hamburg's Chaos Club. In last year's Chaos Congress, they once more held a seminar on Phreaking (given by the Dutch Hac-Tic group; the German report on this part is available, with the Chaos Congress' documentation, either from CCC or from Virus Test Center's ftp site). CCC and Hac-Tic freely distributed information on blue box programs for PCs and 68000 systems. Due to this action, the price of a blue box program went down significantly (from about 500 DM to about 100 DM), and one can upload blue box programs together with games from ordinary BBS. But German Telecom said that the holes which these programs exploit have been patched.

When CAPITAL first contacted me (before the experiment), I was not very impressed. But the the experiment continued, and some really shocking results were reported: when German Telecom could also neither trace nor intercept a second experiment, they reportedly asked some Canadian experts for assistance. When they watched and tried to close the hole, they observed that somebody just worked in their "system" to implant some Trojan horse (don't ask me how, because if I believe Telecom, there is \*\*\*no connection to the outside\*\*\* When they patched the holes in changing some frequencies, this evidently was immediately "mediated" (path unknown) to the phreaks (organised in a group "Dope", evidently working internationally). Unlimited Access comes with a 1-year guarantee of free updates of frequencies: this is different from other blue-boy programs and may verify the unusual price (15,000 DM, about 10,000 \$), but remember that this program excludes being traced by Telecoms! And the group evidently "received" the updated frequencies immediately and distributed them to their "clients".

Just for \*caution and clarification\*: due to the stress of end-of-semester, I couldnot personally observe the experiment. My report is based on some telephone discussions (not bluebox-dialled) with the journalist, on the assessment of a participating colleague which I trust, as well as on some discussions which I had with Telecom on related matters, and with some phreaks in my neighbourhood \*:)

Klaus Brunnstein

# Five `Hackers' Indicted

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 9 Jul 92 11:36:11 PDT

Articles in the NY Times, Washington Post, and elsewhere on 9 July 1992 gave details of federal grand jury indictments on 8 July of five New York City area computer ``hackers". The five, who call themselves ``Masters of Disaster" and ``Masters of Deception" (MOD), are Julio Fernandez, 18 (``Outlaw" --Bronx), John Lee, 21 (``Corrupt" -- Brooklyn), Mark Abene, 20 (``Phiber Optik" -- Queens), Elias Ladopoulos, 22 (``Acid Phreak" -- Queens), and Paul Stira, 22 (``Scorpion" -- Queens). The 11-count indictment accuses the defendants of computer tampering, computer fraud, wire fraud, illegal wiretapping and conspiracy -- including system disruptions and stealing data, including 176 confidential reports on consumers' credit ratings (which they sold), and breaking into computer-communication systems (e.g., a Southwestern Bell 5ESS switch in El Paso, ITT, and TYMNET, Bank of America, Martin-Marietta), credit reporting services (TRW), databases (Trans Union Corp, Information America), and universities (NYU, U.Washington). On Nov. 28, 1989, they allegedly wiped out nearly all of the information in a computer used by the Educational Broadcasting Corp., public television station WNET, Channel 13 in New York. They face up to 5 years in prison for each count, or 55 years in total, plus a maximum fine of \$250,000 for each count. Court-ordered wire-taps were used (apparently the first time for data transfers).

The Times article included this:

In the 11-count indictment, the men were accused of holding a conversation on Nov. 6, 1991, in which they discussed obtaining information on how to alter TRW credit reports adding or removing credit delinquency statements, for example to ``destroy peoples lives or make them look like saints.''

They are also accused of a conversation on Nov. 14, 1991, of discussing a lengthy list of institutions with computers that one of them said, ``We've just got to start hitting these left and right.'' These institutions included government offices, private companies and an Air Force base.

The federal indictment was handed down in Manhattan and was the result of a joint investigation by the U.S. attorney's office, the Secret Service and the FBI.

# "Huge credit card record theft uncovered"

Norm deCarteret 813-878-3994 (TL 438) <normdec@vnet.ibm.com> Sun, 12 Jul 92 19:45:05 EDT

Source: St Petersburg Times, 7/11/92, pg B1, Jane Meinhardt

A Time Inc. employee offered detectives computer records on thousands of credit cards - for a price...on the street for \$1 each

Pinellas County sheriffs detectives on Thursday arrested a Time employee who they said had information on more than 3,000 credit cards, including account numbers, expiration dates...A tipster reported the fraud scheme mid-June to detectives who met the man 4 times...to buy computer discs and lists of credit card numbers...Detectives found additional computer discs and other credit card information in Ferguson's apartment...the data in his apartment would yield information on 80,000 more credit cardholders, Ferguson told Pinellas County's Lt. Rick Wilfong.

"There were credit cards numbers from people all over the country. The detectives made certain requests for credit card numbers from certain regions. He told us he had to manipulate the Time system to get them, and he was able to produce them. He's not a polished criminal in this type of activity. But from what he sold us, he had unusual access to a lot of information he used fraudulently", Marianne Pasha, sheriffs office [...?].

Thomas Ferguson was charged with 4 counts of trafficking in credit cards. "We're reasonably sure he didn't sell to anyone else. He was making attempts to sell to others but we believe we were the first to buy." Wilfong Ferguson had no record of credit card [fraud]. He had been convicted of aggravated assault in 1988...and sentenced to 3 years in prison and one year probation.

Peter Costiglio, Time VP and spokesman:

- Ferguson was a computer analyst for Time for 1.5 years.

- He's been suspended pending the outcome of the criminal investigation.
- Costiglio refused to discuss Fergusons job or Time's security system.

"Any company property has been recovered. There's been no breach of the security system."

That's a reassuring statement? Sigh. Norm deCarteret

#### Kisks quotation

<Jonathan.Bowen@prg.ox.ac.uk> Thu, 9 Jul 92 10:19:58 BST

Recently I found the following quotation that may be of interest to RISKS readers:

"To err is human but to really foul things up requires a computer." -- Farmers' Almanac for 1978 (1977) `Capsules of Wisdom'

This is the only quotation on computers to have made it to `The Oxford Dictionary of Modern Quotations', Oxford University Press, 1991.

Jonathan Bowen, Oxford University

#### Ke: Newsweek Vincennes article (Frankston, <u>RISKS-13.63</u>)

Dan Sorenson <viking@iastate.edu> Thu, 9 Jul 1992 05:49:41 GMT

In the modern battlefield, be it on land or at sea, there is little to no time for a positive visual ID of the incoming. A likely RISK is matching a flight profile or radar pattern to a known threat and firing before being fired upon. In this case, few real details have emerged for armchair analysis. I seem to remember the attacking Japanese flight at Pearl Harbor being dismissed as a flight of friendly, and unarmed, B-17's when spotted on radar. One wonders if the system designer remembered this incident when he wrote the software for the AEGIS system. When there are billions of warship to protect, and civilian lives in the area, which do you choose to protect at all costs?

>One is the image of a technician madly scanning through a dog-eared issue of
>the OAG (the article didn't mention a brand name) to find the Iranian flight.
>It's hard enough to not miss an entry when in a quiet airport in a single time
>zone. I realize that tracking civilian flights was not part of the normal
>battle plan, but I presume that the system has still not been updated to link
>to the civilian airline reservation systems or other such sources of
>information. One change in warfare, which I think the Gulf War illustrated,
>is how the commercial technology has, in many ways, surpassed the military.
>Of course, the online airline info might not be accurate which means a delayed
>flight could still have been missed.

Do not forget that an F-14 or even a B-2 can be listed as a civilian 727 in normal civilian reservation logs. If it was my ship, I wouldn't trust that logbook farther than I could throw it. If it was on an attack profile, I'd open fire. Note that this profile was under investigation for quite a few days, but I don't remember any conclusive findings being published.

>The other is that the tagging of the plane as an F-14 provided for no level >of ambiguity. Even in the heat of battle, can the system cope with multiple >interpretations of data or does it mindless lock in on a worst case and then >present it to the befuddled user as fact?

In a military environment, I would hope so, given the caveat that the user knows it's a worst-case scenario. I always assume a worst-case scenario in my daily network maintainence; would you do less when a warship is at stake?

NOTE: my experience in the Navy has not given me any knowledge of the AEGIS system beyond the general that may be found in Janes. Do not interpret my comments as being those of a technical expert in the AEGIS system.

Dan Sorenson, DoD #1066 z1dan@exnet.iastate.edu viking@iastate.edu

#### 🗡 Re: Airbus

Keith Barr <barr@hickory.mmm.ucar.EDU> Thu, 9 Jul 92 16:50:00 MDT

Below is an excerpt from an article that I posted to rec.aviation, with a cross posting to rec.travel.air, which I didn't notice. The text explains why I am forwarding it to you. Thanks.

BTW the single > are me, and the doubles are [Mark Brader].

>From msb@sq.com Thu Jul 9 16:33:37 1992 To: barrk@tramp.Colorado.EDU Subject: A-320

> I find it rather disappointing -- one has only to read comp.risks for
> a while to gain a distrust of the A-320, or at least its overdose of
> computerization. Starting in November of 1993, when UA's first A-320
> will be delivered, I'll be watching more closely over just what they
> want to put me in.

I think comp.risks readers would be interested in the message you posted in response to the above. I enclose a copy below in case you didn't keep one. You can post to comp.risks by mailing to risks@csl.sri.com.

> As someone who is hoping and praying for a job with UAL someday, I too
> am rather disappointed that United will soon be flying these computerized
> aircraft. I much prefer the Boeing concept of let the computer fly, but
> give the pilot the override capability. I was speaking with a UAL pilot
> Tuesday night about the acquisition, and we chatted about the problems
> of putting all of your eggs in one basket. He told me about two
> Airbus occurences that were interesting, and since I haven't seen them
> mentioned here before, I will post them. I apologize if they are repeats.

> #1 A Pan Am Airbus A300 or A310 (I don't remember which) was on final
> approach in VMC conditions. All was looking well until the airplane
> reached minimums. At that point the aircraft executed a go-around, and
> flew the entire missed approach procedure. The pilots were not able
> to disengage the autopilot until they were well established in the
> hold.

>

#2 Apparently as a safety feature derived from the crash of the
Air Florida flight into the Potomac, a feature was installed on Airbusses
to minimize/eliminate (hah!) the possibility of taking off without full
takeoff thrust. The system automatically pushes the throttles the
rest of the way forward if they are not already there when the nose-wheel
strut decompresses. One time (type and whereabouts unknown to me) an
Airbus was being pushed back from the gate after the pilots had started
both engines. As luck would have it the tow-bar snapped, and the airplane
coasted backwards. When the pilots realized they were just rolling backwards
they stomped on the brakes. The airplane of course, with its aft center of
gravity, tipped back onto it's tail, thus decompressing the nose gear. The
computer took over, and jammed the throttles forward, sending the airplane
racing towards the concourse. The pilots realized what was happening just
in time to avoid a nasty collision with the tug, and terminal building.

> Keith Barr, COMM-AS&MEL/INST/IGI, University of Colorado, Aerospace Engineering
 > barrk@tramp.colorado.edu, barr\_k@silver.colorado.edu, barr@mmm.ucar.edu

# Ke: When Cryptography is Outlawed... (Guntheroth, <u>RISKS-13.63</u>)

<franl@centerline.com> Fri, 10 Jul 92 11:02:16 -0400

Suppose the Federal Government doesn't have trouble decoding encrypted

messages, but wants people to think it does. If so, what's to stop the U.S. from \_loosening\_ restrictions on cryptography? Imagine the risk to privacy in a world where encryption was legal, unrestricted, and widely used in the belief that not even the U.S. government could decipher encrypted messages. In the land of the blind, the one-eyed man is king.

Fran Litterio, CenterLine Software R&D, 10 Fawcett St, Cambridge, MA, USA 02138-1110 franl@centerline.com uunet!centerline!franl 617-498-3255

# **#** Re: When Cryptography is Outlawed... (Guntheroth, <u>RISKS-13.63</u>)

<a\_rubin@dsg4.dse.beckman.com> Thu, 9 Jul 92 13:16:58 PDT

>Perhaps what the Feds are looking for is a new weapon of prosecution; use of

persecution?

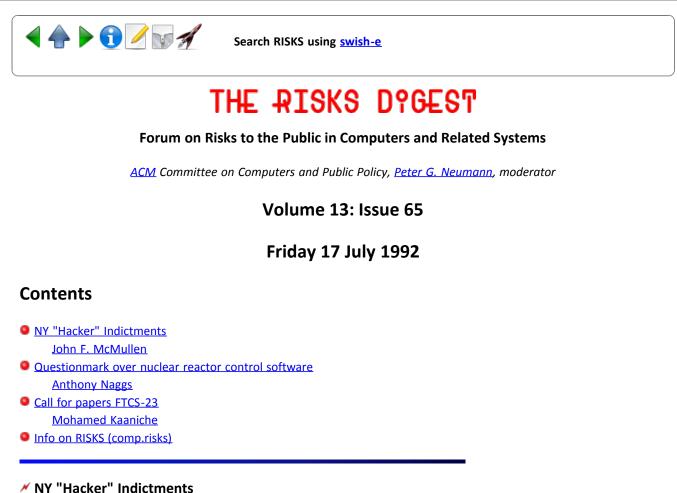
>cryptography is by definition a felony, and widespread use of cryptography
>is then by definition racketeering as defined by RICO. It's like bagging
>Capone for tax evasion, when he was too slippery to be caught breaking the
>law. I find this sloppiness unacceptable as a taxpayer.

Arthur L. Rubin: a\_rubin@dsg4.dse.beckman.com (work) Beckman Instruments/Brea 216-5888@mcimail.com 70707.453@compuserve.com arthur@pnet01.cts.com (personal)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



"John F. McMullen (at Marist)" <KNXD%MARISTB@VM.MARIST.EDU> Fri, 17 Jul 92 13:53:41 EDT

[The following editorial piece is reproduced in full with thanks from Newsbytes, under whose auspices it appeared, and is reprinted with permission of the author(s), including at least John F. McMullen, but possibly also Barbara E. McMullen -- I could not be sure from the context of the double message, one half of which is included here, the other half was an explicitly doubly authored news article. PGN]

Second Thoughts On New York Computer Crime Indictments 7/13/92 NEW YORK, N.Y., U.S.A., 1992 JULY 13 (NB) -- On Wednesday, July 9th, I sat at a press briefing in New York City's Federal Court Building during which law enforcement officials presented details relating to the indictment of 5 young computer "hackers". In describing the alleged transgressions of the indicted, United States Assistant Attorney Stephen Fishbein wove a tale of a conspiracy in which members of an evil sounding group called the "Masters of Destruction" (MOD) attempted to wreck havoc with the telecommunications system of the country.

The accused were charged with infiltrating computer systems belonging to telephone companies, credit bureaus, colleges and defense contractors --Southwestern Bell, BT North America, New York Telephone, ITT, Information America, TRW, Trans Union, Pacific Bell, the University of Washington, New York University, U.S. West, Learning Link, Tymnet and Martin Marietta Electronics

Information, and Missile Group. They were charged with causing injury to the telephone systems, charging long distance calls to the universities, copying private credit information and selling it to third parties -- a long list of heinous activities.

The immediate reaction to the indictments were predictably knee-jerk. Those who support any so-called "hacker"-activities mocked the government and the charges that were presented, forgetting, it seems to me, that these charges are serious -- one of the accused could face up to 40 years in prison and \$2 million in fines; another - 35 years in prison and \$1.5 million in fines. In view of that possibility, it further seems to me that it is a wasteful diversion of effort to get all excited that the government insists on misusing the word "hacker" (The indictment defines computer hacker as "someone who uses a computer or a telephone to obtain unauthorized access to other computers.") or that the government used wiretapping evidence to obtain the indictment (I think that, for at least the time being that the wiretapping was carried out under a valid court order; if it were not, the defendants' attorneys will have a course of action.).

On the other hand, those who traditionally take the government and corporate line were publicly grateful that this threat to our communications life had been removed -- they do not in my judgement properly consider that some of these charges may have been ill-conceived and a result of political considerations.

Both groups, I think, oversimplify and do not give proper consideration to the wide spectrum of issues raised by the indictment document. The issues range from a simple black-and-white case of fraudulently obtaining free telephone time to the much broader question of the appropriate interaction of technology and law enforcement.

The most clear cut cases are the charges such as the ones which allege that two of the indicted, Julio Fernandez a/k/a "Outlaw" and John Lee a/k/a "Corrupt" fraudulently used the computers of New York University to avoid paying long distance charges for calls to computer systems in El Paso Texas and Seattle, Washington. The individuals named either did or did not commit the acts alleged and, if it is proven that they did, they should receive the appropriate penalty (it may be argued that the 5 year, \$250,000 fine maximum for each of the counts in this area is excessive but that is a sentencing issue not an indictment issue.).

Other charges of this black-and-white are those that allege that Fernandez and/or Lee intercepted electronic communications over networks belonging to Tymnet and the Bank of America. Similarly, the charge that Fernandez, on December 4, 1991 possessed hundreds of user id's and passwords of Soutwestern Bell, BT North America and TRW fits in the category of "either he did it or he didn't."

A more troubling count is the charge that the indicted 5 were all part of a conspiracy to "gain access to and control of computer systems in order to enhance their image and prestige among other computer hackers; to harass and intimidate rival hackers and people they did not like; to obtain telephone, credit, information, and other services without paying for them; and to obtain. passwords, account numbers and other things of value which they could sell to

#### others."

To support this allegation, the indictment lists 26, lettered A through Z, "Overt Acts" to support the conspiracy. While this section of the indictment lists numerous telephone calls between some of the individuals, it mentions the ame Paul Stira a/k/a "Scorpion" only twice with both allegations dated "on or about" January 24, 1990, a full 16 months before the next chronological incident. Additionally, Stira is never mentioned as joining in any of the wiretapped conversation -- in fact, he is never mentioned again! I find it hard to believe that he could be considered, from these charges, to have engaged in a criminal conspiracy with any of the other defendants.

Additionally, some of the allegations made under the conspiracy count seem disproportionate to some of the others. Mark Abene a/k/a "Phiber Optik" is of possessing proprietary technical manuals belonging to BT North America while it is charged that Lee and Fernandez, in exchange for several hundred dollars, provided both information on how to illegally access credit reporting bureaus and an actual TRW account and password to a person, Morton Rosenfeld, who later illegally accessed TRW, obtained credit reports on 176 individuals and sold the reports to private detective (Rosenfeld, indicted separately, pled guilty to obtaining and selling the credit reports and named "Julio" and "John" as those who provided him with the information). I did not see anywhere in the charges any indication that Abene, Stira or Elias Lapodoulos conspired with or likewise encouraged Lee or Fernandez to sell information involving the credit bureaus to a third party

Another troubling point is the allegation that Fernandez, Lee, Abene and "others whom they aided and abetted" performed various computer activities "that caused losses to Southwestern Bell of approximately \$370,000." The \$370,000 figure, according to Assistant United States Attorney Stephen Fishbein, was developed by Southwestern Bell and is based on "expenses to locate and replace computer programs and other information that had been modified or otherwise corrupted, expenses to determine the source of the unauthorized intrusions, and expenses for new computers and security devices that were necessary to prevent continued unauthorized access by the defendants and others whom they aided and abetted."

While there is precedent in assigning damages for such things as "expenses for new computers and security devices that were necessary to prevent continued unauthorized access by the defendants and others whom they aided and abetted." (the Riggs, Darden & Grant case in Atlanta found that the defendants were liable for such expenses), many feel that such action is totally wrong. If a person is found uninvited in someone's house, they are appropriately charge with unlawful entry, trespassing, burglary -- whatever the statute is for the transgression; he or she is, however, not charged with the cost of the installation of an alarm system or enhanced locks to insure that no other person unlawfully enters the house.

When I discussed this point with a New York MIS manager, prone to take a strong anti-intruder position, he said that an outbreak of new crimes often results in the use of new technological devices such as the nationwide installation of metal detectors in airports in the 1970's. While he meant this as a justification for liability, the analogy seems rather to support the contrary position. Air line hijackers were prosecuted for all sorts of major crimes; they were, however, never made to pay for the installation of the metal detectors or absorb the salary of the additional air marshalls hired to combat hijacking.

I think the airline analogy also brings out the point that one may both support justifiable penalties for proven crimes and oppose unreasonable ones -- too often, when discussing these issues, observers choose one valid position to the unnecessary exclusion of another valid one. There is nothing contradictory, in my view, to holding both that credit agencies must be required to provide the highest possible level of security for data they have collected AND that persons invading the credit data bases, no matter how secure they are, be held liable for their intrusions. We are long past accepting the rationale that the intruders "are showing how insecure these repositories of our information are." We all know that the lack of security is scandalous; this fact, however, does not excuse criminal behavior (and it should seem evident that the selling of electronic burglar tools so that someone may copy and sell credit reports is not a public service).

The final point that requires serious scrutiny is the use of the indictment as a tool in the on-going political debate over the FBI Digital Telephony proposal. Announcing the indictments, Otto G. Obermaier, United States Attorney for the Southern District of New York, said that this investigation was "the first investigative use of court-authorized wiretaps to obtain conversations and data transmissions of computer hackers." He said that this procedure was essential to the investigation and that "It demonstrates, I think, the federal government's ability to deal with criminal conduct as it moves into new technological areas." He added that the interception of data was possible only because the material was in analog form and added "Most of the new technology is in digital form and there is a pending statute in Congress which seeks the support of telecommunications companies to allow the federal government, under court authorization, to intercept digital transmission. Many of you may have read the newspaper about the laser transmission which go through fiber optics as a method of the coming telecommunications method. The federal government needs the help of Congress and, indeed, the telecommunications companies to able to intercept digital communications."

The FBI proposal has been strongly attacked by the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF) and Computer Professionals for Social Responsibility (CPSR) as an attempt to institutionalize, for the first time, criminal investigations as a responsibility of the communications companies; a responsibility that they feel belongs solely to law-enforcement. Critics further claim that the proposal will impede the development of technology and cause developers to have to "dumb-down" their technologies to include the requested interception facilities. The FBI, on the other hand, maintains that the request is simply an attempt to maintain its present capabilities in the face of advancing technology.

Whatever the merits of the FBI position, it seems that the indictments either would not have been made at this time or, at a minimum, would not have been done with such fanfare if it were not for the desire to attempt to drum up support for the pending legislation. The press conference was the biggest thing of this type since the May 1990 "Operation Sun Devil" press conference in Phoenix, Arizona and, while that conference, wowed us with charges of "hackers" endangering lives by disrupting hospital procedures and being engaged in a nationwide, 13 state conspiracy, this one told us about a bunch of New York kids supposedly engaged in petty theft, using university computers without authorization and performing a number of other acts referred to by Obermaier as "anti-social behavior" -- not quite as heady stuff!

It is not to belittle these charges -- they are quite serious -- to question the fanfare. The conference was attended by a variety of high level Justice Department, FBI and Secret Service personnel and veteran New York City crime reporters tell me that the amount of alleged damages in this case would normally not call for such a production -- New York Daily News reporter Alex Michelini publicly told Obermaier "What you've outlined, basically, except for the sales of credit information, this sounds like a big prank, most of it" (Obermaier's response -- "Well, I suppose, if you can characterize that as a prank but it's really a federal crime allowing people without authorization to rummage through the data of other people to which they do not have access and, as I point out to you again, the burglar cannot be your safety expert. He may be inside and laugh at you when you come home and say that your lock is not particularly good but I think you, if you were affected by that contact, would be somewhat miffed"). One hopes that it is only the fanfare surrounding the indictments that is tied in with the FBI initiative and not the indictments themselves.

As an aside, two law enforcement people that I have spoken to have said that while the statement that the case is "the first investigative use of court-authorized wiretaps to obtain conversations and data transmissions of computer hackers.", while probably true, seems to give the impression that the case is the first one in which data transmission was intercepted. According to these sources, that is far from the case -- there have been many instances of inception of data and fax information by law enforcement officials in recent years.

I know each of the accused in varying degrees. The one that I know the best, Phiber Optik, has participated in panels with myself and law enforcement officials discussing issues relating to so-called "hacker" crime. He has also appeared on various radio and television shows discussing the same issues. These high profile activities have made him an annoyance to some in law enforcement. One hopes that this annoyance played no part in the indictment.

I have found Phiber's presence extremely valuable in these discussions both for the content and for the fact that his very presence attracts an audience that might never otherwise get to hear the voices of Donald Delaney, Mike Godwin, Dorothy Denning and others addressing these issues from quite different vantage points. While he has, in these appearances, said that he has "taken chances to learn things", he has always denied that he has engaged in vandalous behavior and criticized those who do. He has also called those who engage in "carding" and the like as criminals (These statements have been made not only in the panel discussion but also on the occasions that he has guest lectured to my class in "Connectivity" at the New School For Social Research in New York City. In those classes, he has discussed the history of telephone communications in a way that has held a class of professionals enthralled by over two hours. While my impressions of Phiber or any of the others are certainly not a guarantee of innocence on these charges, they should be taken as my personal statement that we re not dealing with a ring of hardened criminals that one would fear on a dark knight.

In summary, knee-jerk reactions should be out and thoughtful analysis in! We should be insisting on appropriate punishment for lawbreakers -- this means neither winking at "exploration" nor allowing inordinate punishment. We should be insisting that companies that have collected data about us properly protect -- and are liable for penalties when they do not. We should not be deflected from this analysis by support or opposition to the FBI proposal before Congress -- that requires separate analysis and has nothing to do with the guilt or innocence of these young men or the appropriate punishment should any guilt be established.

(John F. McMullen/1992 07 13)

(Barbara E. McMullen & John F. McMullen/Press Contacts: Federico E. Virella, Jr., United States Attorney's Office, 212 791-1955; Betty Conkling, United States Secret Service, 212 466-4400; Joseph Valiquette, Jr, Federal Bureau of Investigation, 212 335-2715)

# ✓ Questionmark over nuclear reactor control software

Anthony Naggs <AMN@vms.brighton.ac.uk> Thu, 16 Jul 92 18:05 BST

From the Computer Weekly for Thursday July 16 1992, with full permission (so long as I forward copies of all public responses to the newspaper). The story once again raises the issue of the appropriate use of software on systems that must fail safely.

A couple of background notes:

- 1 Sizewell B is Britain's first PWR (Pressurised Water Reactor), which is currently under construction. A major argument at the planning inquiry in favour of this reactor type was that the design was modern and had a proven track record in the US and elsewhere.
- 2 Nuclear Electric is the rump of the national electricity generating company, the rest was split into two companies and floated on the stock exchange. My understanding is that it owns/operates all British civil nuclear power stations, of various British designs.

I have joined short paragraphs for readability, and all typos are mine.

SAFETY OFFICIALS DOUBT SIZEWELL B SOFTWARE

#### **Tony Collins**

Safety inspectors have questioned the ability of computer protection systems to prevent a major accident at the Sizewell B nuclear power station. They want more reliance on older and trusted solid-state systems without software as a secondary fallback. But Nuclear Electric, Sizewell's operator, is unhappy at the request as it would increase costs - which have already risen from 1,700 million pounds to 2,000 million [times by 2 for US \$]- and could delay Sizewell's launch, set for 1994.

The issue was raised at a recent meeting at the Sizewell site of the Advisory Committee on the Safety of Nuclear Installations. It was also discussed at a British Computer Society safety critical systems task force meeting last week.

It is understood that the Nuclear Installations Inspectorate (NII), part of the Government's Health and Safety watchdog, has asked Nuclear Electric to widen its dependence on magnetic core technology for protection systems. Magnetic core systems, supplied by GEC, have been used for years in UK nuclear power stations and have no programmable software. [Presumably a magnetic core is a device where failure of a current through the core causes control mechanisms to revert to a safe state.]

The move by the NII is a partial victory for computer industry campaigners, who have long argued that public safety should not be entrusted to complex software. Under Nuclear Electric proposals, Sizewell B will be the first nuclear power station in the UK to rely heavily on computers in its primary protection system (PPS), which detects a major failure, and, in the event of an incident, automatically shuts down the power station in a controlled fashion.

But the BCS and other safety-critical software experts say the PPS systems, supplied by US firm Westinghouse, are too complex to test for dependability. The PPS is based on between 300 and 400 Eagle-series microprocessors and 100,000 lines of code.

The NII says it is up to Nuclear Electric to prove that its protection and other systems are safe. Until now inspectors have taken a neutral line, saying they are waiting for all the documentation from Nuclear Electric before deciding on whether the software is safe.

However, officials now indicate that they may refuse to give Nuclear Electric consent to operate Sizewell B, unless the secondary noncomputerised systems provide back-up to all aspects of the computerised PPS.

Nuclear Electric admits that the GEC secondary circuits back-up most, but not all, the computer protection systems. A spokesman for the NII said it has requested, rather than stipulated, that the secondary systems be strengthened. "We have asked them (Nuclear Electric) to consider extending the secondary systems as a prudent measure."

Anthony Naggs, PO Box 1080, Peacehaven BN10 8PZ, Great Britain E-mail: amn@vms.brighton.ac.uk +44 273 589701 (vox)

# Call for papers FTCS-23

<kaaniche@tsf.laas.fr> Fri, 17 Jul 92 17:53:14 +0200

\* FTCS-23 : CALL FOR PAPERS \*

- \* The Twenty Third Annual International Symposium
- \* on Fault-Tolerant Computing
- \* Toulouse, France, June 22-24, 1993
  - \*
- \* Sponsored by IEEE Computer Society and LAAS-CNRS
- \* in cooperation with AFCET and IFIP WG 10.4

# AIMS and TOPICS

The Fault-Tolerant Computing Symposium is the major international forum in computing system dependability. The symposium scope spans system, software and hardware issues, including: architectures, design, implementation, specification, modeling, test, diagnosis, evaluation and validation of dependable and fault-tolerant computing systems.

In addition to regular paper presentations and panel discussions, the symposium offers special sessions on

- i) practical experience in fault-tolerant computing such as design and deployment of a system, failure and recovery field data, and correlation of field data with model predictions,
- ii) innovative ideas in early stages of research and development,
- iii) demonstrations of software tools and systems.

Major topics include, but are not limited to:

- Fault-Tolerant Architectures,
- Fault Tolerance in On-line Transaction Processing Systems,
- Distributed Systems and Real-Time Systems,
- Safety-Critical Systems,
- Software Fault Tolerance,
- Testing and Verification,
- Dependability Modeling and Prediction,
- Defect Tolerance,
- Concurrent Error Detection in VLSI circuits.

# INFORMATION FOR AUTHORS

All submitted material (written in English) will be refereed and should be typed in 1-1/2 spaced, 12 point font. All accepted material will appear in the proceedings.

PAPERS should not exceed 20 pages including figures and text.

PANEL proposals should include the topic(s), a maximum two-page description of the panel objectives, names and addresses of the probable panelists. The

proposed panel chair should include a one-page biographical sketch.

For PRACTICAL EXPERIENCE REPORTS and EARLY INNOVATIVE IDEA REPORTS, the submission should be a 5-10 page description of the experience or the idea. These manuscripts must be marked either "Practical Experience" or "Innovative Idea" for them to be considered in their respective categories.

For SOFTWARE DEMONSTRATIONS, the submission should be a 5-10 page description of the software, its context and objective, and of the planned demonstration. Sun workstations and MacIntoshes connected to a video projector will be available. Please indicate on a separate sheet the requirements for the demonstration. These manuscripts must be marked "Software Demonstration".

#### SUBMISSIONS

Six copies of a 1-page abstract and a list of 5 keywords should be submitted to program chair Ambuj Goyal before October 30, 1992. Mark the envelope "FTCS 23 submission". Abstracts will be used for referee assignments. Please submit your abstracts on time to get best possible reviewing coverage.

Six copies of the papers, panel proposals, practical experience reports, early innovative idea reports and software demonstrations should be submitted to program chair Ambuj Goyal by December 4, 1992 and should be accompanied by ten copies of a title page which includes: the title, author name(s), affiliations, mailing address, phone number, fax number and e-mail, a maximum 150-word abstract, five keywords, an approximate word count and a declaration that the material has been cleared through author affiliations. For multi-authored submissions, the principal contact should be indicated. Mark the envelope "FTCS 23 submission". Submissions arriving late or significantly departing from length guide-lines, or papers published or submitted elsewhere will be returned without review.

Notification of acceptance or rejection of all submissions will be made by March 12, 1993.

#### EXHIBITS

Exhibitors from both industrial and academic communities are encouraged. This will be an opportunity to present advanced products to an informed and sophisticated audience. Proposals must be submitted to exhibits chair Jean-Claude Rault by March 1, 1993 on the official application form available from the exhibits chair.

GENERAL CHAIR: Jean-Claude Laprie (LAAS-CNRS) 7 Avenue du Colonel Roche 31077 Toulouse - France E-mail: Jean-Claude.Laprie@laas.fr

#### PROGRAM COMMITTEE:

CHAIR: Ambuj Goyal IBM T.J. Watson Res. Center P.O. Box 704 Yorktown Heights, NY 10598, USA E-mail: ambuj@watson.ibm.com

V.Agarwal (CDN) J.Hlavicka (CS) D.Lenoski (USA) W.Sanders(USA) R.lyer (USA) J. Arlat (F) Y.Levendel (USA) N.Saxsena(USA) D.Avresky (BG) N.Kanekawa (J) R.Leveugle (F) J.Shen(USA) M.Banatre (F) J.Karlsson (S) M.Malek (USA) S.Shrivastava(GB) P.Banerjee (USA) J.Kelly (USA) G.Masson (USA) D.Siewiorek(USA) D.Blough (USA) K.Kinoshita (J) J.Meyer (USA) L.Simoncini (I) F.Cristian (USA) H.Kopetz (A) B.Smith(USA) T.Nanya (J) T.Dahbura (USA) T.Krol (NL) M.Nicolaidis (F) Y.Tamir(USA) C.Georgiou (USA) J.Lala (USA) D.Powell (F) D.Taylor(CDN) J.Gray (USA) G.Le Lann (F) S.Reddy (USA) H.Wunderlich(D)

CONFERENCE COORDINATOR

Marie-Therese Ippolito (LAAS-CNRS) E-mail: Marie-Therese.Ippolito@laas.fr

PUBLICATION CHAIR

David Powell(LAAS-CNRS) E-mail: David.Powell@laas.fr

PUBLICITY CHAIR

Mohamed Kaaniche(LAAS-CNRS) E-mail: Mohamed.Kaaniche@laas.fr

EXHIBITS CHAIR

Jean-Claude Rault (EC2) 269 rue de la Garenne 92024 Nanterre - France Tel +(33) 1 47 80 70 00 Fax +(33) 1 47 80 66 29

**EX OFFICIO** 

Jacob Abraham, FTC-TC Chair The University of Texas at Austin 2201 Donley Drive Austin, TX 78758 - USA jaa@cerc.utexas.edu

FOR FURTHER INFORMATION and/or a copy of the advance program when available, contact:

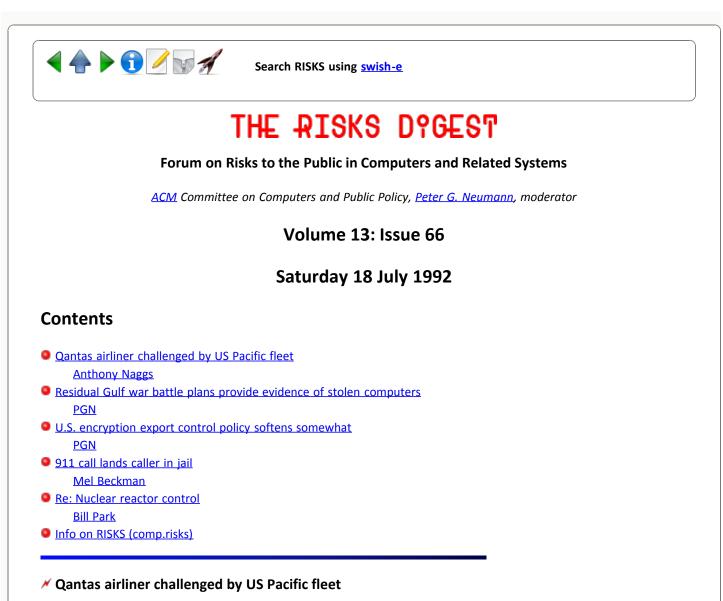
Mohamed Kaaniche LAAS-CNRS 7 Avenue du Colonel Roche 31077 Toulouse - France E-mail: Mohamed.Kaaniche@laas.fr Tel +(33) 61 33 64 05 Fax +(33) 61 33 64 11

Mohamed KAANICHEemail: kaaniche@laas.frLAAS-CNRStel: +33 / 61.33.64.057 av du colonel Rochefax: +33 / 61.33.64.1131077 TOULOUSE CedexFRANCE



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# Anthony Naggs <AMN@vms.brighton.ac.uk>

Thu, 16 Jul 92 0:35 BST

[I'm not sure about the degree of computer influence here, but I thought it would fit with the discussion here about the Vincennes attack on the Iranian airliner. The following item appeared on page 11 (International News) of the British national newspaper The Guardian, on Wednesday July 15 1992, attributed to Reuters in Canberra.]

# QANTAS AIRLINER THREATENED BY US NAVY WARSHIP

A US warship threatened yesterday to shoot down an Australian airliner with more than 300 passengers over the Pacific. The pilot of Qantas flight QF12, an hour out of Los Angeles on its way to Sydney, was jolted by a call from the warship saying he faced "hostile action" if the aircraft did not leave the area, a Qantas spokesman said.

The US Navy's Pacific Fleet in Pearl Harbour later identified the ship as the USS Cowpens, the same class of Aegis missile cruiser as the USS Vincennes which shot down an Iranian civilian airliner in the Gulf in July 1988, killing 290

people.

The Qantas pilot radioed the Federal Aviation Authority in Los Angeles which put him on a frequency to the warship. [Why was this necessary?] The FAA resolved the crisis by putting the Qantas flight on a path bypassing the Cowpens which was taking part in a military exercise.

Elly Brekke, a spokeswoman for the FAA in Los Angeles, confirmed that the airliner, following its predetermined flight path, was told it risked risked facing hostile action. Ms Brekke said the Qantas flight was "where it should have been", and the FAA had not been told that the US Navy was conducting manoeuvres that would require any restriction of airspace.

The Pacific Fleet spokesman said the Cowpens had inadvertently [!] used "an international distress frequency" in trying to contact planes taking part in the exercise.

"We're looking into how it happened", Commander Jim Kudla said. He also said the exercise commander had taken measures to ensure the incident would not happen again. [How do you prevent something from recurring if you don't know how it happened before?]

Anthony Naggs, PO Box 1080, Peacehaven BN10 8PZ, Great Britain E-mail: amn@vms.brighton.ac.uk +44 273 589701 (vox)

### Residual Gulf war battle plans provide evidence of stolen computers

"Peter G. Neumann" <neumann@csl.sri.com> Sat, 18 Jul 92 15:52:23 PDT

About \$70,000 worth of computers used in the Persian Gulf operations turned up for sale in Ventura County, CA. An unidentified computer hobbyist reported observing `Welcome to Saudi Arabia' on the screen of one computer, along with a map and locations of unit deployments. He reported it to the Crime Stoppers hotline. Subsequent Army investigators have now led to the conviction of a serviceman for multiple counts of larceny and wrongful disposition of government property. [There was some residual military information in some of the computers, although no indication was given as to whether any of it was sensitive.] [Los Angeles Daily News item, in San Francisco Chronicle, 17 July 1992, p.E6]

# ✓ U.S. encryption export control policy softens somewhat

"Peter G. Neumann" <neumann@csl.sri.com> Sat, 18 Jul 92 16:05:01 PDT

The Bush administration has agreed to ease export controls on encryption-based software somewhat. In the battle between NSA's desires to be able to intercept international communications and software vendors' desires to be able to compete in international markets, this decision transfers control of encryption software to the Commerce Department (from the State Department). Evidently,

systems that work with up to 40-digit RSA keys will now be eligible for export, although one can already buy much better stuff on the streets of in Europe -- for example, Cryptos, which uses both DES and RSA, is available in Moscow! In addition, the administration will now meet with industry representatives up to twice a year. [Source: Don Clark, San Francisco Chronicle, 18 July 1992, p.B1]

#### 🗡 911 call lands caller in jail

Mel Beckman <mbeckman@mbeckman.mbeckman.com> Sat, 18 Jul 92 11:47:06 PST

In this morning's Ventura County Star/Free Press newspaper (Sat 92jul17) appears an article headlined "Woman calls for help, lands in jail." Here is my own summary of their story (cross-posted to comp.society.privacy):

Oxnard, CA resident Helene Golemon called 911 to report (twice) a loud teenage street party in the wee hours. Later, at 6:00am, an officer arrived and arrested her on a (subsequently learned-to-be) erroneous misdemeanor traffic warrant.

Golemon expressed outrage at the 911 records check, and that the warrant even existed at all. "Those kids were out there drinking and driving drunk. Nothing happened to them and I got arrested." After booking, including fingerprints and mug shots, she was detained in a holding cell until her husband posted \$188 bond later that morning.

Assistant police chief William Cady claimed that dispatchers often check available records, even on a reporting person, to know as much as possible about the people involved when responding to 911 calls. "Procedurally, our people did nothing wrong" he said.

The arrest warrant, dated from an illegal left turn from May, 1988. Golemon fought the ticket and lost, then attended state-sponsored driver's education (a CA alternative to fines available for first-time offenders) in August 1988. The court has a copy of Golemon's driver education certificate on file, and Linda Finn, deputy executive officer for Ventura County Superior and Municipal Courts, couldn't explain why a warrant was later issued in 1989. Golemon was never notified of the warrant.

Goleman felt the incident was vindictive, because the dispatcher was annoyed with her. "When I tried to explain the continuing problems we're having, she was very short with me," she said. Golemon then asked for the dispatchers name, and the dispatcher in turn demanded Golemon's full name. After Golemon complied, the dispatcher only told Golemon her badge number. The dispatcher remains unidentified in the news report, and an Oxnard police sergeant who reviewed the tape said the dispatcher was "absolutely professional."

The privacy and computer risk concerns here seems to me three fold.

First, the police often act with inappropriate gravity on erroneous, and apparently unverifiable, data. Under what circumstances does a misdemeanor warrant demand a 6:00am public arrest? Certainly more time could have been

expended verifying the data, as an at-large illegal left-turner hardly threatens public safety.

Second, apparently innocuous -- even beneficial -- contacts with government can result in record searches for unrelated information. Not only may this result in egregious seizures, as in this case, but such an atmosphere can only stultify public/government relations. Crime and corruption thrive in such an environment.

Third, although individuals have the right to know most information the government retains on them (FOIA), that right becomes meaningless if the government can, at any time, decided to integrate facts from disjoint data bases and then act without notice on resulting conclusions. One cannot submit an FOI request on the union of multiple far-flung data sets!

Mel Beckman, Beckman Software Engineering, 1201 Nilgai Place, Ventura, CA 93003 Compuserve: 75226,2257 805/647-1641 mbeckman@mbeckman.com

# Ke: Nuclear reactor control (Re: <u>RISKS-13.65</u>)

Bill Park <park@netcom.com> Fri, 17 Jul 92 18:33:40 PDT

> "Magnetic core systems, supplied by GEC, have been used for years in UK ...

I think rather that "magnetic core systems" probably refers to a early type of electrical signal amplification device -- the magnetic core amplifier or MCA. They have been used since at least the 1950s in the highly-critical control systems of U.S. nuclear submarines, and, I suppose, in nuclear power plants as well. They are little-known and somewhat "old-fashioned" devices now, much like fluidic devices -- remember them? Much faster, smaller, lighter, more efficient and less expensive semiconductor devices are widely available these days that are reliable enough for many critical uses.

An MCA is super-reliable because it is simple: just two coils of wire on an iron core, like a transformer. The ancient Romans could have made one. It has no moving parts, no connections that open and close sputtering arcs of metal vapor as do relays, and no semiconductors to fail when their part per billion impurities finally migrate far enough to cause a short or reduce gain. As long as the insulation on its wires holds up, an MCA can't do anything \*but\* work correctly. Don't make smoke come out of it and it'll literally last forever.

#### Simplified Theory of MCA Operation:

One of the coils in an MCA has many turns, is driven with direct current (DC), and is the input, or controlling coil. The other, output coil has relatively few turns, and is placed in series with an alternating-current (AC) load to be controlled, such as an AC motor. With no current through the controlling coil, a rapidly-varying magnetic field produced by the iron core induces a "bucking" voltage in the output coil that that opposes any current that tries to flow through the load, turning it "off."

To turn on the load, put a relatively weak DC current through the controlling coil. This drives the magnetization of the iron so far in one direction that it "saturates" (all magnetic domains are aligned in the same direction and the iron is fully magnetized). Although the magnetic field in the iron is still very strong, it is now constant instead of varying, so it no longer induces any bucking voltage, and current can flow almost unimpeded through the load, turning it "on." The larger number of turns in the input coil allows a small current through it to overcome any demagnetizing forces produced by the load current flowing through the output coil.

By combining MCAs with solid-state rectifiers (though not necessarily semiconductor ones -- the Romans could have made them, too), and by wiring them in cascade, large amplifications are possible. MCAs can also exert proportional control over the power to a load. Bridge circuits enable bidirectional control.

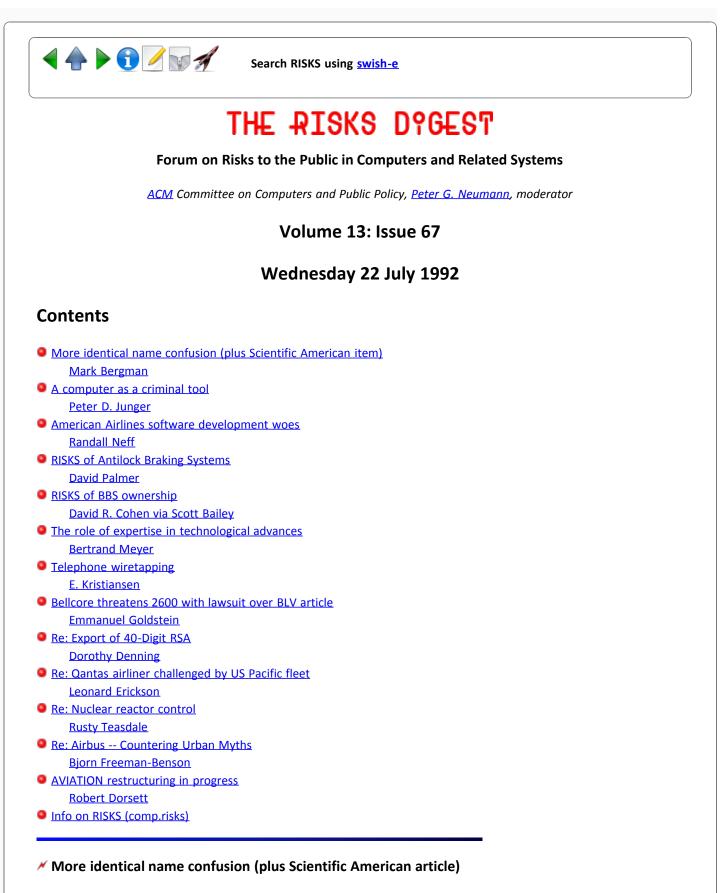
Individual MCAs in a control system may be very reliable, but that does not mean the system will fail safe if one of the MCAs fails. A classic dilemma from robotics is, "Should the robot freeze or go limp if something fails?" If it freezes while it is reaching inside a car body going by on a conveyor belt, the car body will collide with the arm. But if the arm goes limp, it can fall (or sag down) onto something breakable, or drop something heavy.

Moral: Look at the whole system. Murphy will.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mark Bergman <bergman@panix.com> Wed, 22 Jul 92 1:03:51 EDT

Here is another story from the AP wires about health service computers and name

collisions. (There is also an article in this month's Scientific American, "Achieving Electronic Privacy," by David Chaum, about encryption and smart card transactions to ensure privacy \_and\_ verify each side to the transaction.) I don't feel qualified to comment, but I'd like to hear other people's thoughts. Mark Bergman 718-855-9148 {cmcl2,psi,uunet,apple}!panix!bergman

Computer Confuses Babies With Same Name, Denies Benefits to One

PENSACOLA, Fla. (AP) - A Pensacola woman says her 5-month-old daughter cannot get state social service benefits because a computer has her child confused with a St. Petersburg baby with the same name. The children, both named Samantha Marie Morris, were born only eight days apart but are linked by a maze of computer glitches haunting the Florida Department of Health and Rehabilitative Services. The Pensacola baby isn't getting food stamps or Medicaid benefits, her mother, Tina Morris, said Monday. "If my daughter had an emergency, got sick or something, some places might take it, but they wouldn't pay for it," she said. "I've been real lucky. She hasn't been sick."

The HRS' balky new \$104.2 million computer thinks she is the St. Petersburg Samantha, eligible for the same benefits and listed with the same Social Security number, the Pensacola mother said. HRS District Administrator Chelly Schembera said she was unfamiliar with the case. She said the computer problems that have been affecting the agency across the state exceeded normal start-up glitches for a new system.

Ms. Morris said she spent two days at the local HRS office trying to clear up her daughter's problem without success and that her case worker has been trying since April. The computer problems have caused Ms. Morris and other HRS clients to wait in long lines. She said she waited 20 minutes outside under a hot sun to get food stamps last week for the rest of her family and once in the building was told it would take another hour.

Schembera said the agency is considering lemonade stands, extra chairs, awnings, baby changing tables and play rooms to help clients bear the long waits.

One man already has capitalized by setting up a snack stand outside an HRS building in Pensacola, accepting food stamps as payment. "This guy could be fairly wealthy by the time the crisis is over," Schembera said.

#### A computer as a criminal tool

Peter D. Junger <Junger@samsara.law.cwru.edu> Tue, 21 Jul 1992 22:19:05 GMT

In the Cleveland Plain Dealer for July 21, 1992 a story appears with a headline nearly worthy of the National Enquirer.

The headline is: POLICE PULL PLUG ON COMPUTER IN MORALS STING The byline is: By DEBORAH A. WINSTON, PLAIN DEALER REPORTER The venue is: MUNROE FALLS

[I've lived in Cleveland for over twenty years and have never heard of Munroe Falls--that's how small it is. It turns out that it is in Summit County, Ohio, near Akron.]

The story suggests that there is an especial risk to having computers in a very small, Midwestern town.

According to the story, the Munroe Falls police received a complaint that a local electronic bulletin board "containing sexually explicit material might be accessible to children."

So the police set up a sting operation, using a local 15 year-old boy as their agent. The story goes on to say: "After the youth was able to hook into the bulletin board, police arrested Mark Lehrer, 22, owner and operator of Akron Anomaly, a 1,000 member bulletin board." And the police also seized all of Lehrer's computer--apparently on the ground that it was "criminal tools."

[From talking to the reporter and Lehrer's lawyer, I found out that Lehrer was indicted today "of disseminating matter harmful to juveniles and possession of criminal tools," with the criminal tools being the computer.]

It seems that Lehrer's bulletin board included some gif files containing pictures of James Bond and Captain Kirk and subjects like that, which could be downloaded by subscribers. There were also some gif files that were supposed to be accessible only by adults over the age of 18. The article reports, however, that: "when police seized Lehrer's records they found that even the `clean' files contained images that were not entirely wholesome." [Lehrer's attorney told me that these were files that had been uploaded to the bulletin board and had not yet been seen by Lehrer.]

The article then quotes the Munroe Falls Police Chief as saying of these "not entirely wholesome files": "One was Bugs Bunny eating a carrot, one was Bart Simpson riding a skateboard and one was called (a slang term for oral sex), and that was in the clean file." There were apparently also some pictures of naked women and of "naked women engaging in sexual acts" that were not in the adult category.

According to the article, the Police Chief also said that "it's possible that some of the games and movies are being accessed in violation of copy right laws."

And then there is a final direct quote from the Police Chief: "I'm not saying it's obscene because I'm not getting into that battle, but it's certainly not appropriate for kids, especially without parental permission."

Peter D. Junger, Case Western Reserve University Law School, Cleveland, OH Internet: JUNGER@SAMSARA.LAW.CWRU.Edu -- Bitnet: JUNGER@CWRU

#### American Airlines software development woes

Randall Neff <neff@mandor.Metaphor.COM> Wed, 22 Jul 92 09:22:19 PDT

[San Jose Mercury News, Monday, July 20, 1992 Business Monday section p. 9F]

Software nightmare comes alive for airline American finds the pieces of new reservation system do not fit together

[Dallas Morning News] DALLAS -- AMR Corp. for decades sliced up competition with its Sabre computer system for making airline reservations. Last week, the parent of American Airlines, Inc. said it fell on its sword trying to develop a state-of-the-art, industry-wide system that could also handle car and hotel reservations.

AMR cut off development of its new Confirm reservation system only weeks after it was supposed to start taking care of transactions for partners Budget Rent-A-Car, Hilton Hotels Corp. and Marriott Corp. Suspension of the \$125 million, 4-year-old project translated into a \$165 million pre-tax charge against AMR's earnings in the second quarter and fractured the company's reputation as a pacesetter in travel technology.

"In an area where we arguably are one of the world's leading companies, it's particularly disappointing to us when we have to recognize a loss of that magnitude on that kind of activity," said ARM senior vice president and treasurer Michael J. Durham. The disappointment comes after a series of technical and management missteps that surprised not only AMR, but the entire industry. As far back as January, the leaders of Confirm discovered that the labors of more than 200 programmers, systems analysts and engineers had apparently been for naught. The main pieces of the massive project -- requiring 47,000 pages to describe -- had been developed separately, by different methods. When put together, they did not work with each other.

The system was based on twin IBM mainframes that stored the two main pieces of the reservation system, according to project leaders. One IBM 3090 computer stored customer records, pricing information, and other "decision support" data. The other IBM 3090 kept track of available rooms and cars, managing the actual transaction. But the two pieces were developed on different operating systems. When the developers attempted to plug the parts together, they could not. Different "modules" could not pull the information needed from the other side of the bridge. Response times were slow on other requests.

Not until April did officials begin to "recognize the magnitude of the situation" and begin to realize that the problems might not be under control. Warnings of lengthy delays -- as much as two years -- began to surface. "Somewhere in there, you've got a management problem," said Donald Tatzin, director of Arthur D. Little's travel consulting practice.

AMR Information Services fired eight senior project members, including team leader John Mott, saying it had "determined that information about the true status of the project appears to have been suppressed by certain management personnel." In late June, Budget and Hilton said they were dropping out.

For the record, AMR said it was not giving up hope of salvaging Confirm, although a Coopers & Lybrand market study for AMR is believed to cast doubt on its viability.

# RISKS of Antilock Braking Systems

David Palmer <palmer@cco.caltech.edu> Thu, 16 Jul 1992 15:56:53 GMT

The 15 July 1992 Washington Post has an article about one side effect of Antilock Braking Systems (ABS).

Accident investigators typically estimate how fast the various vehicles involved in a collision were going by looking at the skid marks left behind. However, with ABS systems, the skid marks are faint, intermittent, and not as durable as conventional skidmarks. (ABS works by releasing the brakes whenever the tires start skidding. Therefore, the tires never get a chance to cook a strip of rubber into the asphalt.)

The skid marks are visible, if you look carefully and get to the accident site before they've been worn away by rain and other traffic.

Thus, the new technology makes it harder to reconstruct accidents.

The article did, however, quote one investigator as saying (paraphrased from memory) that he'd rather see faint skid marks for 45 feet than dark skid marks for 55 feet ending at a wall.

David Palmer, Goddard Space Flight Center/NASA palmer@tgrs.gsfc.nasa.gov

#### RISKS of BBS ownership (From David R. Cohen, forwarded)

Scott Bailey <SBAILEY@xcc.mc.xerox.com> Wed, 22 Jul 1992 06:28:00 PDT

I found this posted in one of the Star Trek newsgroups (!). Looks like interesting RISKS material to me.

Scott Bailey Xerox Computer Center sbailey@xcc.mc.xerox.com Webster, NY

X-NEWS: oasis rec.arts.startrek.misc: 1583

Relay-Version: VMS News - V6.0-1 14/11/90 VAX/VMS V5.5; site oasis.xcc.mc.xerox.com Path: oasis.xcc.mc.xerox.com!rocksanne!rochester!rutgers!cs.utexas.edu!uunet!

zaphod.mps.ohio-state.edu!magnus.acs.ohio-state.edu!usenet.ins.cwru.edu! cleveland.Freenet.Edu!bx953

Newsgroups: rec.arts.startrek.misc

Subject: Help, please forward this message

From: bx953@cleveland.Freenet.Edu (David R. Cohen)

Date: 21 Jul 92 14:09:03 GMT

I have no idea where this message should be posted, I only know that it \*\*should\*\* be posted. I'm posting here only because I know this board is widely read and someone should be able to get this message to the right place.

In [the 21 July 1992] Cleveland Plain Dealer, it was reported that a 22-year old male got arrested for distributing pornography, and possibly for contributing to the delinquency of a minor. His "crime" was running a bulletin board out of his home ... the cops found out that minors were able to get ahold of pornographic gif files. The arrestee had apparently set things up so that "adult" files were supposed to be restricted, but either the files weren't restricted after all, or someone else had "unrestricted" them. The paper reports that this type of arrest is one of the first of its kind in the state. The cops used a "cooperative" 15 year old -- after the kid accessed the adult files, the cops grabbed the alleged criminal.

If any Ohio law enforcement types are reading this, I am an Ohio attorney, and I think this sucks.

David David R. Cohen or Tracey L. Ridgeway bx953@cleveland.freenet.edu

# M The role of expertise in technological advances

Bertrand Meyer, Interactive Software Engineering <bertrand@eiffel.com> Sun, 19 Jul 92 18:30:08 PDT

This note is a call for argued opinions about the effect of technological advances on the value of people's expertise and qualifications. In particular it would be interesting to hear views about the relative merits of the following two opposite conjectures:

A. The introduction of a new technology gives the highest advantage to people who are already the most advanced experts, as they are in the best position to understand the new developments, and thus will benefit the most from them. The advances will in face increase the lead that the best people already had over the others.

B. Introducing a new technology makes it possible for many people to do what was previously the exclusive specialty of a few experts. So it levels off the field, putting everyone at the same position.

I can see serious arguments and examples supporting both conjectures. To keep this note short, I have selected just two widely different examples, one for each. Only the second is computer-related. (My personal interest in this discussion is with respect to advances in software engineering, but the problem is more general.)

A. In his book ``Tristes Tropiques", the ethnologist Claude Levi-Strauss recounts how he visited a South American tribe that didn't know writing. He introduced it to them; writing was immediately put to good use by the tribe's chief, who could see how the ability to record and retrieve his decisions would increase his power.

B. It used to be quite hard to get a taxi in Paris. The situation has considerably improved thanks to the installation by the biggest taxi company of a computer-based system. This might at first seem to be an argument for A since this system has (at least temporarily) given the company a big lead over its competitors, but here is the other side. In a recent stay in Paris in which I frequently needed taxis to pick me up, I was able almost every time to obtain one in about five minutes. I once complimented a driver on this efficiency. He responded by heaping tons of abuse on the system. After a period of astonishment, I understood the reason for his anger. He has been in the business for twenty years or so, and knows every street and lane in the city; he also knows the best itineraries, and where he should and should not be at each time of day and year to get good business (go to the Gare d'Austerlitz at certain times, to the airports at certain others and so on). But now the new system puts every upstart driver, who has just passed his exam and paid for his license, at the same level as him! You just key in a certain code to indicate where you are, and get queued for customers' requests in that area. Then when your turn comes you get the next customer. The computer system apparently also indicates where the hottest areas are at any time of day. Very little advantage remains for an experienced professional driver. He was looking with even more horror to a future (apparently promised) extension of the system, whereby ``the computer'' would show recommended itineraries!

Please note that the discussion is not about people whose job is simply made obsolete by the new advances (as craftsmen at the time of the industrial revolution, or draughtsmen at the time of the introduction of computer-aided design). Assuming people are experts in a field, and remain in that field, is new technology a way to increase their lead or should they fear losing their advantage?

[Please respond directly to Bertrand, who will share the results with us. PGN]

# ×

Date:Wed, 22 Jul 92 09:16:03 CETFrom: "E. Kristiansen - WMS" <EKRISTIA@estec.estec.esa.nl>Subject:Telephone wiretapping [Cross-posted to privacy@cv.vortex.com]

NRC Handelsblad, a Dutch newspaper, of 20 July has two articles concerning telephone wiretapping.

The first article describes several cases of alleged unauthorized wiretaps performed by PTT Telecon, the Dutch telephone company. The PTT is accused of establishing wiretaps on telephone lines without the required court order, on request of the police and legal authorities (district attorney). In one case, a PTT employee has allegedly passed on information obtained from illegally bugging a phone line, to a criminal (drug dealer). The employee has been fired. A PTT spokesperson says that "according to current procedure", the police cannot request a wiretap directly. The request is to be submitted through the proper legal channels. From a technical point of view, the article suggests, without giving much detail, that it is very easy to establish a wiretap, and that the only control is through procedures, relying on "highly trusted personnel". Further, it is said that the PTT never performs wiretapping itself, it only establishes the tap to a line going to the police office. It is not said that the PTT CANNOT do wiretapping, and I would assume that they can, e.g. for technical monitoring of line quality.

The other article describes how an on-hook telephone set can be used for bugging the room in which it is installed. The trick can be performed by anybody who can gain access, legally or illegally, to any point of the wire pair connecting the telephone set to the exchange. A high frequency signal is injected into the line. This signal bypasses the hook switch of the set (capacitive coupling, I suppose). The microphone modulates the signal (technical details not given), and the intruder can demodulate, and listen to the conversation in the room. When this trick was published in the press, PTT says it will shortly be offering a telephone plug with a built-in capacitor to short the HF signal. The plug will sell for about Dfl.5 (USD 3). Consumer organizations urge that the plug should be available free of charge to anybody asking for it. It is not said whether the trick will work on all current types of phones, or only on particular brands. Erling Kristiansen

Bellcore threatens 2600 with lawsuit over Busy Line Verification item

Emmanuel Goldstein <emmanuel@well.sf.ca.us> Wed, 22 Jul 92 09:07:20 -0700

THE FOLLOWING CERTIFIED LETTER HAS BEEN RECEIVED BY 2600 MAGAZINE. WE WELCOME ANY COMMENTS AND/OR INTERPRETATIONS.

Leonard Charles Suchyta General Attorney Intellectual Property Matters

Emanuel [sic] Golstein [sic], Editor 2600 Magazine P.O. Box 752 Middle Island, New York 11953-0752

Dear Mr. Golstein:

It has come to our attention that you have somehow obtained and published in the 1991-1992 Winter edition of 2600 Magazine portions of certain Bellcore proprietary internal documents.

This letter is to formally advise you that, if at any time in the future you (or your magazine) come into possession of, publish, or otherwise disclose any Bellcore information or documentation which either (i) you have any reason to believe is proprietary to Bellcore or has not been made publicly available by Bellcore or (ii) is marked "proprietary," "confidential," "restricted," or with any other legend denoting Bellcore's proprietary interest therein, Bellcore will vigorously pursue all legal remedies available to it including, but not limited to, injunctive relief and monetary damages, against you, your magazine, and its sources.

We trust that you fully understand Bellcore's position on this matter.

Sincerely,

LCS/sms

[The 2600 article in question will not appear in RISKS, for the obvious reasons. PGN]

# 🗡 Export of 40-Digit RSA

Dorothy Denning <denning@cs.georgetown.edu> Wed, 22 Jul 92 14:45:34 EDT

I talked with Dennis Branstad at NIST and found out that the 40-digit system approved for export is not the RSA public-key system (PKS) but rather the systems RC-2 and RC-4 which are single-key systems marketed by RSA Data Security. These systems can be "married to" a 512-bit RSA PKS used for key management and the whole package can be exported. Dorothy Denning

[Dorothy and I had an earlier off-line dialogue on the fact that 40-digit RSA was child's-play to break. This clarification is very helpful. PGN]

# Ke: Qantas airliner challenged by US Pacific fleet (<u>RISKS-13.66</u>)

Leonard Erickson <leonard@qiclab.scn.rain.com> Mon, 20 Jul 1992 04:28:42 GMT

>The Qantas pilot radioed the Federal Aviation Authority in Los Angeles which >put him on a frequency to the warship. [Why was this necessary?] The FAA >resolved the crisis by putting the Qantas flight on a path bypassing the >Cowpens which was taking part in a military exercise.

It was probably necessary to use such a roundabout means of communication because the airliner had no idea what frequencies the ship was using, and likely \*couldn't\* respond on many of them if it wanted to!

>Elly Brekke, a spokeswoman for the FAA in Los Angeles, confirmed that the >airliner, following its predetermined flight path, was told it risked risked >facing hostile action. Ms Brekke said the Qantas flight was "where it should >have been", and the FAA had not been told that the US Navy was conducting >manoeuvres that would require any restriction of airspace.

Somebody goofed. My guess is the military \*should\* have warned the ATC center!

>The Pacific Fleet spokesman said the Cowpens had inadvertently [!] used "an >international distress frequency" in trying to contact planes taking part in >the exercise.

The inadvertently part is all too simple. And it has bearing on my comment above about why the airliner may not have been able to directly contact the ship.

All those nice agreements about which frequencies are used for what have a \*large\* loophole. All governments are allowed to ignore the international frequency allocations when it comes to \*military\* use.

Most military gear can tune all sort of civilian (and other) frequencies. And for peacetime operations, they do have the civilian frequencies set up. Somebody may have done something as simple as punch the wrong "general frequency" button! There are two risks here. First, from the pictures that I've seen of military radio gear, the "user interface" is lacking in a few areas. Mainly in that the user has no idea that some of the "channels" are not strictly military.

The second risk is the usual one of what happens when folks that are allowed to "ignore the standards" get to share the operating environment with folks that \*do\* have to follow them...

Leonard Erickson leonard@qiclab.scn.rain.com 70465.203@compuserve.com CIS: [70465,203] FIDO: 1:105/56 Leonard.Erickson@f56.n105.z1.fidonet.org

### Ke: Nuclear reactor control (Park, Re: <u>RISKS-13.66</u>)

Rusty <rteasdal@polyslo.csc.calpoly.edu> Mon, 20 Jul 92 18:08:28 GMT

I suspect that, given the context in which they were mentioned, that Bill is correct. However, what I first think of when the phrase "magnetic core systems" comes up in discussions of reactor safety is something rather different. It is the practice in many PWR reactors to have the cadmium control rods, which must be withdrawn partly from the reactor core for substantial fission to take place, lifted vertically up and out of the core by electromagnets, which are themselves powered by the output of the generators driven by the reactor. If there is a sudden drop in reactor output for some reason, the magnets cut out, and the rods drop back into the core. Gravitic passive safety! However, this does not help at all in cases where the reactor is running out of control but still producing steam and power, nor will it do any good if something has happened to prevent the reinsertion of the damper rods themselves...

Russ Teasdale -- rteasdal@polyslo.CalPoly.EDU -- (Rusty)

### Countering Urban Myths re: Airbus

Bjorn Freeman-Benson <bnfb@ursamajor.UVic.CA> Thu, 16 Jul 92 11:00:44 PDT

In <u>RISKS 13.64</u>, I read these two stories about the A320: <> #1 A Pan Am Airbus A300 or A310 (I don't remember which) was on final ... <> #2 Apparently as a safety feature derived from the crash of the ...

And I immediately recalled that the same article was posted to sci.aeronautics and then immediately countered as a collection of Urban Myths. I'm sorry that I cannot quote the sci.aeronautics article, but the local news system has already erased it.

Not a fan of the A320, yet also a crusader against misinformation, Bjorn N. Freeman-Benson

### AVIATION restructuring in progress

Robert Dorsett <rdd@rascal.ics.utexas.edu> Tue, 21 Jul 92 18:13:35 CDT

Rec.aviation is currently in the request-for-discussion period of a comprehensive re-organization proposal. A number of proposed sub-groups may be of interest to RISKS users, including two airliners proposals (in the sci and rec hierarchies), a safety-group, a generic airplane-group, and others.

The RFD was posted last week; a "survey" of user preferences (which will be used to shape the final CFV) was posted about the same time. The survey was re-posted this afternoon.

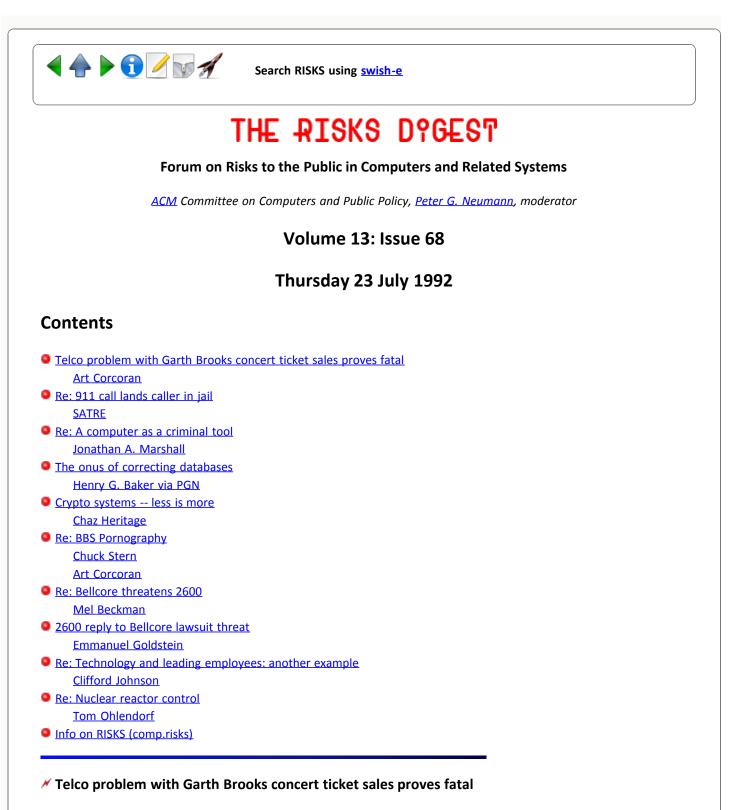
Copies of both documents are available on rec.aviation, sci.aeronautics, and rec.travel.air, depending on your news spool. Copies may also be obtained from me, directly, at rdd@rascal.ics.utexas.edu.

Robert Dorsett, Internet: rdd@rascal.ics.utexas.edu UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Art Corcoran <corcoran@tusun2.mcs.utulsa.edu> Thu, 23 Jul 1992 16:36:46 -0500

Our local (Tulsa, OK) television news reported today about how a telco problem proved fatal. A retired Doctor [Homer Hardy] tried to call 911 when his wife [Phyllis Joan Love Hardy, 67] started having a heart attack. His 7-8 attempts always resulted in a busy signal. He finally dialed 0 for the operator, but when the ambulance arrived, his wife was already dead. It seems the telco was overloaded with over 320,000 calls in one hour by persons trying to buy tickets to a concert by country musician, Garth Brooks.

One of the persons in the story commented, "I guess Garth Brooks tickets are more important than 911 service."

Art Corcoran, University of Tulsa, corcoran@tusun2.mcs.utulsa.edu

[Also noted by Phil Karn <karn@thumper.bellcore.com>. An AP story noted that the number of calls exceeded the previous record for Tulsa BY A FACTOR OF TWO. Promoters sold out 23,000 tickets within three hours in Tulsa and Oklahoma City to two Brooks' concerts. Now they will have to do Garthroscopic surgery on the phone system. PGN]

### Ke: 911 call lands caller in jail (Beckman, <u>RISKS-13.66</u>)

RGB Technology/703-556-0667 <SATRE@cisco.nosc.mil> Mon, 20 Jul 1992 06:35 PDT

Mel Beckman reports that "CA resident Helene Golemon called 911 to report (twice) a loud teenage street party in the wee hours." The risk being identified is the police looking up the resident's criminal record. How about the much more serious risk of tying up 911 with a non-life threatening call?

#### Ke: A computer as a criminal tool (Junger, <u>RISKS-13.67</u>)

Jonathan A. Marshall <marshall@cs.unc.edu> Thu, 23 Jul 92 11:27:42 -0400

Would it be safe to assume that the 15-year-old had his parents' permission to participate in the sting and access the adult files? His parents might have known that he could encounter adult pictures during the sting. If so, then perhaps their permission means that no crime actually occurred during the sting, and the case could be thrown out.

--Jonathan A. Marshall, Computer Science, UNC-Chapel Hill, marshall@cs.unc.edu

### M The onus of correcting databases (From Henry G. Baker)

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 23 Jul 92 17:34:31 PDT

Here is an excerpt from a SnailMail letter from Henry G. Baker:

I have recently been trying with only moderate success to correct my credit file at the Equifax credit reporting organization based in Atlanta. As you may have seen on the news, they have settled with a number of states' attorneys general over their sloppy data.

After getting a copy of my report, and noticing a large number of entries that looked suspiciously as if they belonged to someone else, and seeing one of my previous addresses as ``25 Roycroft Dr.'' (I never lived on that street, nor do I even know where it is), I asked Equifax to remove the entry. The first letter to Equifax didn't work, but a combination of a second letter from me and one from my lawyer finally produced a correction to my file: I am now listed as having previously lived on ``25 Cancel Dr.''!!

By the way, Equifax also listed my marital status as ``single'', even though it (correctly) listed my wife's name in the ``spouse'' section, along with her (correct!) social security number.

I think that I have now been sensitized to the problem of unfettered national databases, and words like ``radicalized'' and ``click'' come to mind. (Am I dating myself?)

[I hope you are not dating yourself, especially as you are married. PGN]

Nimble Computer Corp., 16231 Meadow Ridge Way, Encino CA 91436, 818-501-4956

#### 🗡 Crypto systems -- less is more

<chaz\_heritage.wgc1@rx.xerox.com> Thu, 23 Jul 1992 09:43:37 PDT

There has been much discussion recently on RISKS about the FBI's demands to be allowed to tap phones, etc. and about the restrictions, proposed and implemented, on the export from the USA of cryptological apparatus, whether hardware or software.

If one wants - as a bank might - to encipher all of a large volume of transmissions then this is certainly an important issue; the security and 'exportability' of systems like DES and RSA would clearly be mission-critical in these circumstances.

However, the justification for these restrictive measures is said to be to facilitate policing. It is said, for example that phone-taps are vital to the 'war on [untaxed] drugs', and encryption restrictions to the fight against terrorism.

Any competent criminal or terrorist obliged to use his own telephone would naturally expect it to be tapped, whatever Constitutional 'rights' he might believe himself to have, and act accordingly; if he were obliged to send a co-conspirator a note about their conspiracies then they would doubtless arrange beforehand a secure cipher system.

The Foreign Office one-time pad system is said never to have been broken, and those who know far more about cryptology than I do seem to think that it never will be. It is easy to generate its key, and relatively easy to use it for short messages. A simple modification of the system does not rely on the physical transfer of key, eliminating the possibility of detection in transit.

The FBI therefore seem to have little chance of catching anyone competent, since they will probably not intercept meaningful conversations between serious crooks, and will be unable to break FO one-time pad cipher should the villains choose to use it.

All they will do is hasten the natural selection of criminals and terrorists until only those who are really professional (and therefore dangerous) will still be in business, filling the prisons meanwhile with small fry and amateurs who have, perhaps, been foolish enough to trust their telephones and their expensive, but crippled, commercial cipher systems.

What, then, is the true purpose of demanding new phone-taps and restrictions on encryption technology?

This for me is merely a matter of curiousity, since I am British, and therefore prohibited by the criminal law from attempting to transmit any form of code or secret writing (our spooks got this sorted out in the time of the \*first\* Queen Elizabeth).

Baffled, Chaz

### Ke: BBS Pornography (Cohen, <u>RISKS-13.67</u>)

Chuck Stern <chuck@novus.com> Thu, 23 Jul 1992 09:52:14 -0400

This is in partial response to a posting by Mr David Cohen (bx953@cleveland. freenet.edu) concerning the recent Akron-area BBS bust.

Put your money where your mouth is. Not just Mr. Cohen, but anyone who thinks that arrests of this sort are anything less than savory. If you are an attorney, donate some time to write an Amicus brief for the court, if such things are allowed for criminal prosecutions. Even better, if the miscarriage of justice is so great that it makes you want to scream, donate some time to help defend the case. If you have some knowledge, share it with elected officials who are making the laws without the benefit of technical expertise.

Remember that the government never willingly grants a right, or even a privilege, to its citizens. And in these days of the "War on Crime", we must protect what rights we have.

Chuck Stern chuck@novus.com

#### Ke: BBS Pornography (Cohen, <u>RISKS-13.67</u>)

Art Corcoran <corcoran@tusun2.mcs.utulsa.edu> Thu, 23 Jul 1992 17:00:09 -0500

We have had at least two cases of BBS Porn here in Tulsa. The local news even had a three part "expose" on the subject last summer. I attended a sysop meeting at the time. "People in the know" said (i.e., rumored) that the sysop's computer equipment is impounded for over six months and that it is often "dropped" or otherwise damaged by the authorities.

Computers cannot sue for "Police brutality".

In one of the cases, a woman was reading a message and called police when "foul

language was uncontrollably displayed on her screen". (That is, she was offended by the contents of the message.)

Art Corcoran, University of Tulsa, corcoran@tusun2.mcs.utulsa.edu

### Ke: Bellcore threatens 2600 (Goldstein, <u>RISKS-13.67</u>)

Mel Beckman <mbeckman@mbeckman.mbeckman.com> Thu, 23 Jul 92 09:07:07 PST

As someone who has also been involved in of 2600's dubious reprints, I feel reasonably qualified to respond. In the September 1987 issue, 2600 printed a facsimile of an internal technical document I wrote while employed as an IBM systems developer. The document explained how to decrypt password security on the IBM S/36 (the encryption is trivial although not obvious). The document was intended as a "worksheet" for accessing systems where the original "security officer" (superuser) password has been lost or forgotten. With this article, anybody could gain superuser access to a S/36. I still don't know how 2600 got the thing, but my copyright (the series of technical notes is personally copyrighted by me; not a work-for-hire) was stripped off (according to 2600, before they received the document), although my name was still on the thing.

At the time of reprinting, I had left the original job and was working at another company (NEWS 34-38 magazine, a technical journal covering the IBM S/34/36/38 systems). I found out about the problem when a lawyer from IBM's Rochester, MN development lab called me, quite irate, wanting to know why I had publicized this document. The way 2600 presented my document -- with no explanation how it was received -- it looked like I had submitted the thing for publication!

The noise being made by IBM was causing all kinds of problems for me. My current employer was concerned about possible adverse publicity accruing to one of its regular authors and editors; the original firm doing IBM systems programming was none too happy and let it be known that the problem was all mine; my already tentative relationship with IBM's Rochester lab certainly didn't improve (some relationships were definitely cut off by this incident) and I had to spend a huge amount of time talking with everybody, including the lawyers, trying to convince them I hadn't instigating the incident.

2600 was, in my opinion, irresponsible in printing something with a persons name on it, without making any attempt to contact me (I'm in many online directories, including nic & Compuserve). If they couldn't contact the author, the ethical thing to do is not publish. 2600 apparently couldn't resists such a "juicy" tidbit though, whatever the cost to somebody else. As this was a titled document -- and obviously part of a series -- 2600 reasonably could deduce that somebody owned the thing and that permission should be obtained. At that time, presumption of copyright wasn't a legal doctrine (although now, thankfully, it is), however, 2600 should know that lack of a copyright notice doesn't mean that the notice wasn't illegally removed. Their claim to be able to publish the contents as a news item anyway is academic, as they published a photographic facimile of my work. I also thought 2600 should have withheld the document on the simple grounds that public disclosure would put a good deal of small business systems at exposure to attack. We all know that 2600 revels in making public information that can compromise security, to the great embarassment of system manufacturers (hopefully coercing mfrs into improving their products). Somewhere, though, in a democratic society, there is a line that separates mature activism from juvenile vandalism. 2600 crossed that line in my situation.

I had little legal recourse against 2600, and the editor (at that time, Eric Corley), insisted in phone discussions that I was greatly exaggerating my problems. He never apologized, although I did get from him a promise to not further publish anything with my name without permission.

I think there is a place for publications such as 2600 (I regularly pick up a copy at Reiters Technical Books in Washington, DC), but 2600 goes over the line periodically, as they did in my case and possibly in the Bellcore case at hand (I haven't seen '91 winter issue). Since Emmanuel asked for comments on his Bellcore lawyer letter, I figured some history from "one of us" could help provide perspective. I consider myself a open-minded member of the Internet community, on the CPSR/EFF side of privacy and information freedom issues, but I nevertheless take exception to some of 2600's practices.

Mel Beckman, Beckman Software Engineering, 1201 Nilgai Place, Ventura, CA 93003 805-647-1641 mbeckman@mbeckman.com Compuserve: 75226,2257 Fax: 805/647-3125

As background, following are the two letters exchanged by my magazine's attorneys and Eric Corley.

-----

April 15, 1988 Blah, blah & blah Law Offices

Eric Corley, Editor/Publisher Peter Kang, Office Manager 2600 MAGAZINE Middle Island, NY

Dear Sirs:

I have been asked to contact you on behalf of Mel Beckman and his employer, NEWS 34-38 magazine. It is my understanding that your publication, 2600 Magazine, for the month of September 1987, included the publication of confidential memorandum written by Mr. Beckman while he was an employee of another company. The name of the article was "Decrypting Password Security."

We do not know how the memorandum came into your possession, but its unauthorized use may do serious damage to Mr. Beckman's reputation and to that of his current employer. No determination has yet been made as to what steps may be taken to protect the interests of Mr. Beckman and NEWS 34-38. In the meantime, demand is hereby made that you desist from any further unauthorized use of any articles or documents produced by Mr. Beckman. Please confirm in writing that you will comply with this demand.

Very truly yours,

[attorney's signature]

-----

May 31, 1988

Dear [attorney's name]

These are the facts as I know them regarding the acquisition by 2600 Magazine of the article entitled "Decrypting Password Security" written by Mel Beckman.

In August of 1987 we received a copy of the article on a single sheet of paper. There was no indication of a copyright or clues to the article being a "confidential memorandum". No company name was evident and there was no publication from which to ask permission for reprinting. The only identification mark on the entire page was the name "Mel Beckman" which was unknown to us.

Our magazine is in the habit of printing interesting and humorous pages from telephone books, non-copyrighted manuals, and books that we happen to be reviewing. We do not print personal memos or anything else that would invade the privacy of any one person. Given the facts as they were presented to us at the time we believe no wrongful action was taken on our part. I might also point out that had we indeed managed to track down the author and been refused permission to reprint the article, we would still be able to reveal the contents as a news item, since the article had been leaked to us. But let us not delude ourselves--the article was not all that earth-shattering.

We strongly doubt any harm will come to Mr. Beckman's reputation as a result of this incident. Obviously some other person is responsible for sending the article to us. Mr. Beckman cannot and should not be held accountable for another person's actions.

You can rest assured that any future articles we may receive with Mr. Beckman's name on them will not be reprinted in our magazine.

Sincerely,

Eric Corley, Editor, 2600 Magazine

### 2600 reply to Bellcore lawsuit threat

Emmanuel Goldstein <emmanuel@well.sf.ca.us> Thu, 23 Jul 92 15:33:25 -0700

The following reply has been sent to Bellcore. Since we believe they have received it by now, we are making it public.

Emmanuel Goldstein Editor, 2600 Magazine PO Box 752 Middle Island, NY 11953

July 20, 1992

Leonard Charles Suchyta LCC 2E-311 290 W. Mt. Pleasant Avenue Livingston, NJ 07039

Dear Mr. Suchyta:

We are sorry that the information published in the Winter 1991-92 issue of 2600 disturbs you. Since you do not specify which article you take exception to, we must assume that you're referring to our revelation of built-in privacy holes in the telephone infrastructure which appeared on Page 42. In that piece, we quoted from an internal Bellcore memo as well as Bell Operating Company documents. This is not the first time we have done this. It will not be the last.

We recognize that it must be troubling to you when a journal like ours publishes potentially embarrassing information of the sort described above. But as journalists, we have a certain obligation that cannot be cast aside every time a large and powerful entity gets annoyed. That obligation compels us to report the facts as we know them to our readers, who have a keen interest in this subject matter. If, as is often the case, documents, memoranda, and/or bits of information in other forms are leaked to us, we have every right to report on the contents therein. If you find fault with this logic, your argument lies not with us, but with the general concept of a free press.

And, as a lawyer specializing in intellectual property law, you know that you cannot in good faith claim that merely stamping "proprietary" or "secret" on a document establishes that document as a trade secret or as proprietary information. In the absence of a specific explanation to the contrary, we must assume that information about the publicly supported telephone system and infrastructure is of public importance, and that Bellcore will have difficulty establishing in court that any information in our magazine can benefit Bellcore's competitors, if indeed Bellcore has any competitors.

If in fact you choose to challenge our First Amendment rights to disseminate important information about the telephone infrastructure, we will be compelled to respond by seeking all legal remedies against you, which may include sanctions provided for in Federal and state statutes and rules of civil procedure. We will also be compelled to publicize your use of lawsuits and the threat of legal action to harass and intimidate.

Sincerely, Emmanuel Goldstein

Ke: Technology and leading employees: another example (Meyer, <u>RISKS-13.67</u>)

"Clifford Johnson" <Cliff@Forsythe.Stanford.EDU> Thu, 23 Jul 92 16:24:51 PDT

> [Technological] advances will in face increase the lead that

> the best people already had over the others.

In many (especially large) organizations, the presumption that the best have a lead over their co-workers is untrue. Ever heard the parable of the cave-dwellers putting out the eyes of the one who could see?

# Ke: Nuclear reactor control (Teasdale, Re: <u>RISKS-13.67</u>)

"Tom Ohlendorf - TSU Admin. DP, (410) 830-3642" <D7AP002@TOA.TOWSON.EDU> Thu, 23 Jul 1992 08:45 EDT

My particular reply is to the statement:

> However, this does not help at all in cases where the reactor
> is running out of control but still producing steam and power, nor will it do
> any good if something has happened to prevent the reinsertion of the damper
> rods themselves...

While I am not even close to an expert in the nuclear power industry, I did work for a firm that made security systems for nuclear power plants and had an opportunity to learn something about the operations of the industry.

Based on my acquired knowledge, the reason why operators and computer systems monitor the reaction is to prevent a run-away reaction such as cited above. The computer systems are sophisticated enough to be able to SCRAM (or drop the control rods for those that don't know what SCRAMing is) the reactor when the reaction goes out of control. The human monitors also have this control in case the computer fails.

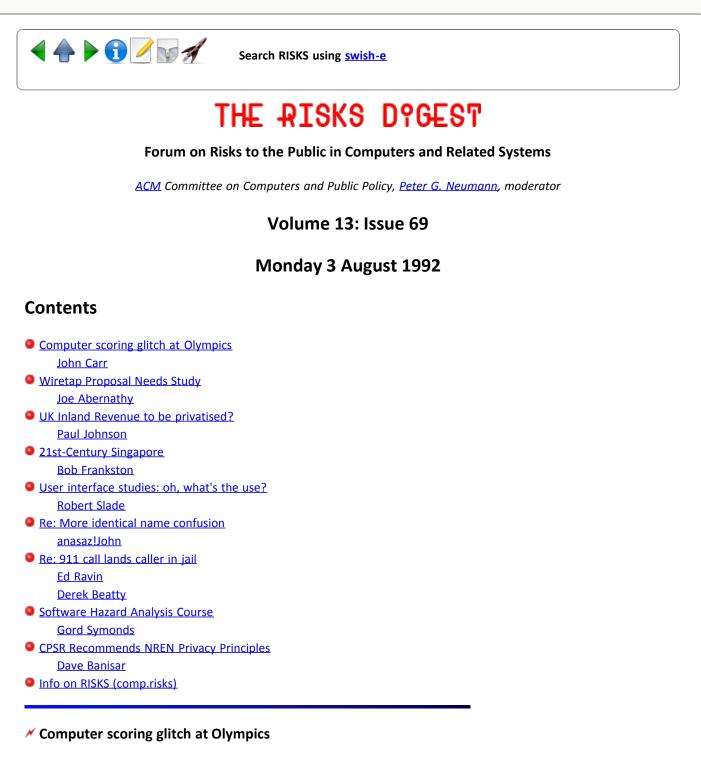
BTW, for you trivia buffs, SCRAM stands for Secondary Control Rod Axe Man. In the days before all of the sophisticated control, a person would have to physically cut the control rod cable with an axe when a reaction went run-away.

Tom Ohlendorf, Programmer/Analyst INTERNET: D7AP002@TOA.TOWSON.EDU



Search RISKS using swish-e

Report problems with the web pages to the maintainer



John Carr <jfc@Athena.MIT.EDU> Sun, 02 Aug 1992 16:17:00 EDT

Excerpts from an article in the August 2, 1992 Boston \_Globe\_:

"Judges Not Quick to Punch; Computer KO's Griffin"

BADALONA, Spain -- Science lied yesterday.

Five judges watching American light flyweight Eric Griffin fight Spaniard Rafael Lozano ... said the gold medal favorite had advanced as expected into the quarterfinals. Three said he did it by a wide margin. ...

A computer said differently.

The computer lied.

What the computer insisted ... was that Eric Griffin was a 6-5 loser. And for the moment at least, that decision will stand, regardless of the opinion of the five men who actually watched the fight. ...

Actually, after a review of the scorecards, it seemed more like some kind of computer glitch, but the result was the same. Elimination of a fighter. Destruction of a dream. Sorry about that. ...

Under the scoring system, at least two judges must hit a button that registers a scoring point within a second after the first judge does. If the do not, the point is not awarded by the main frame computer, even though each point will be recorded individually.

The individual judges scored the match 10-9, 26-17, 18-9, 19-10, and 8-5.

The article said the system was installed after a Korean fighter won a victory at the 1988 olympics even though general opinion was that he lost the fight. [Later stories indicate the appeal failed. PGN]

### Wiretap Proposal Needs Study

Joe Abernathy <chron!ecopy501!edtjda@uunet.UU.NET> Fri, 31 Jul 92 15:25:39 CDT

[AP excerpts by Joe, from an article by W. Dale Nelson, 30 Jul 1992]

Changes in wiretapping laws proposed by the FBI need further work, said Rep. Edward J. Markey, D-Mass, Chairman of the House subcommittee on telecommunications and finance. (In May, the FBI called for legislative changes to enable it to tap into new technologies such as cellular and ISDN.) Markey said a report by GAO "shows that more work needs to be done before the FBI's proposals can be seriously considered by the Congress. ... Before we impose wholesale changes on the communications industry, we must understand the details of what the FBI needs for each technology, and how those needs can be met with minimal costs to consumers and minimal threat to the telephone network."

The GAO said it could not answer questions about the impact of the FBI proposals on costs, benefits and alternatives until the FBI had more clearly defined its specific needs. It also said the least intrusive alternatives could not be determined until the telecommunications industry had received and analyzed information on the FBI's needs. It said the correct solutions "will vary with the technology" but its analysis of the technological alternatives had been classified by the FBI and could not be disclosed.

The budget submitted to Congress by the FBI in February included \$26.6 million to update eavesdropping techniques.

#### ✓ UK Inland Revenue to be privatised?

paj <paj@gec-mrc.co.uk> 24 Jul 1992 09:08:23-BST

I heard on Radio 4 today that the UK government is considering farming out the Inland Revenue's computer operations to a private company. Currently the IR spend 250M pounds per year on computing and hold some 40M files. 5 possible contractors are being approached, including IBM, DEC and ICL.

A union representative gave a long list of reasons why this was a bad idea, starting with confidentiality. He claimed that the IR has a good reputation on this, and worried that a commercial company might not be as honest. The government either was not represented or did not comment.

Paul Johnson (paj@gec-mrc.co.uk). | Tel: +44 245 73331 ext 3245

#### 21st-Century Singapore

<Bob\_Frankston@frankston.com> Tue 28 Jul 1992 10:34 -0400

>From "World Press Review" quoting "China Daily", Beijing [!]:

The government of Singapore has announced a plan to link all households through grids of fiber-optic cables that will allow high-speed exchanges of text, sound, video and other media. The project called the National Information Infrastructure (NI), will also include a wireless communications network to give mobile-computer users access to information services. The NII is part of Singapore's drive to become a world leader in information and communications technology, which officials see as the backbone of 21st-century economies. Towards this end, all citizens 18 and older have been issued identity cards that allow government ministries and other bodies to cross-index information about them.

#### ✓ User interface studies: oh, what's the use?

Robert Slade <rslade@cue.bc.ca> 31 Jul 92 16:04 -0700

To bank to make deposits and withdrawal for lunch money. Chat with neighbour while Sweet Old Thing (i.e., my age) dithers with machine. Murmur from SOT: "Oh, dear. I have to make a deposit." Neighbour points out "deposit" key. More chat with neighbour. Murmur from SOT: "Does the stripe go up?" Neighbour points out picture of card (showing orientation) above slot. More chat with neighbour. Murmur from SOT: "It's still not going it." (ATM has by this time, shut down.)

(Still need to deposit and withdraw. Look at lineup for tellers. Recall last time I used "manual" cashier: no lineup at cashier, five people in line for ATM. Thought I was really smart until realized that all five people at ATM have completed transactions before I got my money. Decide to eat at "golden arches".) Go to Skytrain station. Couple (of SOTs) at next ticket machine looking very worried. Take bill from wallet. Accidentally tear bill. Replace bill in wallet, take other. Complete transaction with ticket machine. Couple at next machine: "How do you work this?" Point out large legend at top. A: look at map, check how many zones to cross; B: push button for number of zones (machine displays price); C: put money in (pictures of acceptable coins over coin slot, acceptable bills over bill slot); D: take ticket. Point out large A by map, B by buttons, etc. Couple goes back to worrying in front of next ticket machine.

Recall study on data base interface. Experimental systems: two commercial systems, three diverse experimental interfaces, one super-deluxe-easy-to-use-never-meant-to-be-implemented-because-\*too\*-easy-and-takes-too-much-processing-power-to-run inteface. Super-deluxe is natural language interface. Results show no benefit from any system. Further (frantic) investigation reveals subjects, normal data base users, cannot consistently make query in own native language.

Become very depressed.

Vancouver Institute for Research into User Security, Vancouver, Canada V7K 2G6 ROBERTS@decus.ca Robert\_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

#### Ke: More identical name confusion (Bergman, <u>RISKS-13.67</u>)

<anasaz!john@enuucp.eas.asu.edu> Thu, 23 Jul 10:05:19 1992

> The HRS' balky new \$104.2 million computer thinks she is the St.Petersburg
 > Samantha, eligible for the same benefits and listed with the same Social
 > Security number, the Pensacola mother said. ..

It looks to me like there is another risk here. HRS paid \$104.2 million dollars for that system! There is simply no excuse for spending this much money on such a system. This is the risk of letting government agencies buy computer systems... not only do they not work.... they also cost too much!

### Re: 911 call lands caller in jail

Unix Guru-in-Training <elr%trintex@uunet.UU.NET> Sat, 25 Jul 1992 03:46:32 GMT

In <u>RISKS-13.68</u>, <SATRE@cisco.nosc.mil> implies that the "risk of tying up 911 with a non-life threatening call" is much more serious than the jailing of a woman who called 911 to complain about a loud street party. Alas, in many big cities, if you want a police officer to appear at the scene, you MUST dial 911. Let's take New York City as an example --

Here's what happens if I call 911 about an incident: the 911 operator types in the address where I am reporting an emergency, then types in my description of

the problem. The report is then sent onward (as a computer message) to the dispatcher for the police precinct in question. The report appears on the dispatcher's screen, who finds an available police car and reads the report over the radio to the police officers who will handle the "job".

If any person in this chain of events screws up --- if the police officer never shows up, if the dispatcher never calls a police car, etc., the responsible party can usually be determined by following the computer audit trail. The computer system also tracks the status of the report and I've often heard dispatchers radioing police officers asking them about the status of "jobs" that were resolved hours ago but were not cleared in the computer. When there are too many reports that have not had officers sent to them, the dispatcher announces an "alert" in the precinct and the officers race to finish up their current "jobs" and get to the new ones.

The result is that there is a fair amount of machinery keeping track of a call to the police. But if I call my local precinct directly with a non-life threatening situation, a bedraggled desk officer will answer the phone, take my complaint, and then, if he or she feels like it, call 911 in order to get a car dispatched. If the desk officer doesn't feel like sending a car right away, they might type the complaint into the dispatch system as a "past complaint" job, and someone MAY get around to acting upon it much later that evening. Worst of all, the desk officer has the option of simply ignoring my complaint, and there is no mechanism (apart from me calling back again when I see no one has acted upon my call) to detect that he has done so. I've found that if I want the police to respond to nuisances like car alarms or street disputes, I have to call 911.

The computer-human interface that is at the core of so many emergency dispatch systems has other quirks, too. In New York City, one sad side-effect of the "alert" mechanism described above is that the dispatcher will start assigning multiple jobs to the same patrol car in order to convince the computer that the precinct is no longer in "alert" status. Never mind that officers in the same car cannot be in two places at once, or that they might be diverted before they can handle the second "job" -- it keeps the computer happy.

Ed Ravin, Prodigy Services Company, 445 Hamilton Avenue, White Plains, NY 10601 elr@trintex.UUCP philabs!trintex!elr +1-914-993-4737

### ×

Derek Beatty <beatty+@cs.cmu.edu> Sat, 25 Jul 1992 11:53:03 -0400 (EDT)

RGB Technology/703-556-0667 <SATRE@cisco.nosc.mil> (...) asks about the "much more serious risk of tying up 911 with a non-life threatening call." This points out another risk: that of using systems in ways not originally intended. 9-1-1 service was originally for emergencies only (or so I believe). But it turns out that the \*only\* way to have a police car dispatched in Pittsburgh is to call 911. Calling the neighborhood police station (5 blocks away!) doesn't work---they direct you to call 911. I suppose there's also a risk here that a distributed system (local police stations) has been replaced by one with a single point of failure. I also wonder whether if I called the local station about an imminent threat whether they'd respond, or just say "call 911."

Derek\_Beatty@cs.cmu.edu (No NeXTmail! MIME Ok.) PhD student 412 268-7898 Computer Science, Carnegie Mellon Univ., 5000 Forbes Ave, Pgh PA 15213 USA

#### Software Hazard Analysis Course

Gord Symonds <GRSYMONDS@HPB.HWC.CA> Fri, 24 Jul 1992 07:38:31 -0400 (EDT)

DLSF Systems Inc. will be presenting a Software Hazard Analysis Course which will include practical insight, procedures and guidelines, 24-26 August 1992, in Ottawa, Ontario. For further information, please contact DLSF Systems Inc., Susan Fraser, (613) 592-8188 (voice), (613) 592-2167 (FAX). Must register by 14 August.

### ✓ CPSR Recommends NREN Privacy Principles

Dave Banisar <banisar@washofc.cpsr.org> Fri, 24 Jul 1992 17:28:43 EDT

CPSR Recommends NREN Privacy Principles (24 Jul 1992)

WASHINGTON, DC -- Computer Professionals for Social Responsibility (CPSR), a national public interest organization, has recommended privacy guidelines for the nation's computer network. At a hearing this week before the National Commission on Library and Information Science, CPSR recommended a privacy policy for the National Research and Education Network or "NREN." Marc Rotenberg, Washington Director of CPSR, said "We hope this proposal will get the ball rolling. The failure to develop a good policy for the computer network could be very costly in the long term."

The National Commission is currently reviewing comments for a report to the Office of Science and Technology Policy on the future of the NREN. Mr. Rotenberg said there are several reasons that the Commission should address the privacy issue. "First, the move toward commercialization of the network is certain to exacerbate privacy concerns. Second, current law does not do a very good job of protecting computer messages. Third, technology won't solve all the problems."

The CPSR principles are (1) protect confidentiality, (2) identify privacy implications in new services, (3) limit collection of personal data, (4) restrict transfer of personal information,(5) do not charge for routine privacy protection, (6) incorporate technical safeguards, (7) develop appropriate security policies, and (8) create an enforcement mechanism.

Professor David Flaherty, an expert in telecommunications privacy law, said "The CPSR principles fit squarely in the middle of similar efforts in other countries to promote network services. This looks like a good approach."

Evan Hendricks, the chair of the United States Privacy Council and editor of

Privacy Times, said that the United States is "behind the curve" on privacy and needs to catch up with other countries who are already developing privacy guidelines. "The Europeans are racing forward, and we've been left with dust on our face."

The CPSR privacy guidelines are similar to a set of principles developed almost 20 years ago called The Code of Fair Information practices. The Code was developed by a government task force that included policy makers, privacy experts, and computer scientists. The Code later became the basis of the United States Privacy Act.

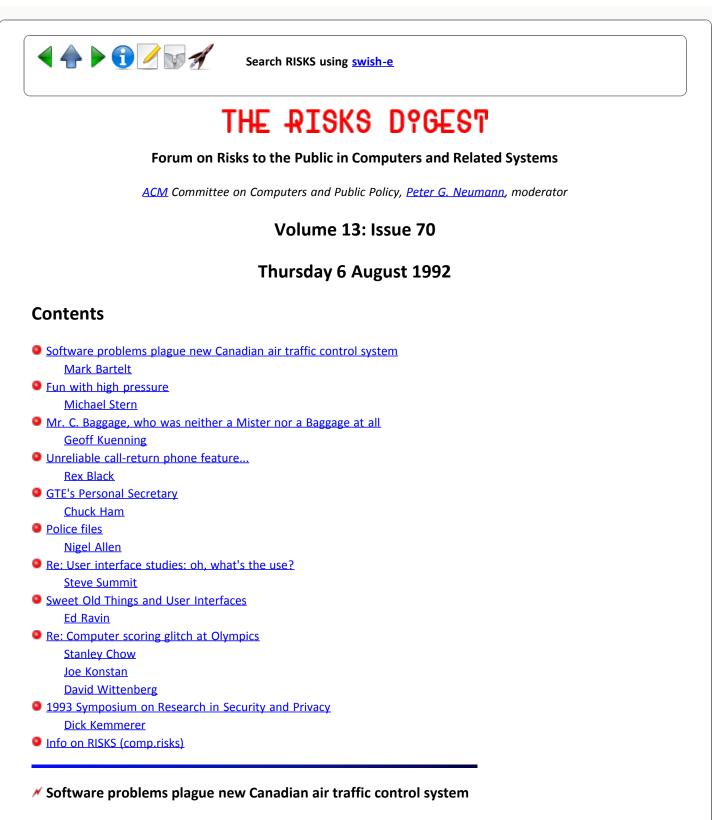
Dr. Ronni Rosenberg, who has studied the role of computer scientists in public policy, said that "Computer professionals have an important role to play in privacy policy. The CPSR privacy guidelines are another example of how scientists can contribute to public policy."

CPSR is a membership organization of 2500 professionals in the technology field. For more information about the Privacy Policies and how to join CPSR, contact CPSR, P.O. Box 717, Palo Alto CA 94302. 415/322-3778 (tel) and 415/322-3798 (fax). Email at cpsr@csli.stanford.edu.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mark Bartelt <sysmark@mouse.cita.utoronto.ca> Tue, 4 Aug 92 06:49:37 EDT

Glitches stalling updated airport radar Bugs mar new air control system Toronto Star, 3 August 1992 By Bruce Campion-Smith An \$810 million program to install updated radar systems at Canada's major airports has been stalled by a series of stubborn software bugs. The sophisticated system has crashed in tests and in actual use, freezing radar screens, displaying false information and even showing jets flying backwards, sources say. In at least one case, air traffic controllers in Montreal were left without radar for 15 minutes when the system suffered a "catastrophic failure," according to federal documents.

Controllers restricted flights and later that March night resorted to the old radar system, according to a memo obtained by The Star under the Access to Information Act. At no time were passengers at risk, says a letter accompanying the memo.

"It's incredible. It's a multi-million-dollar operation. We're up to version four and it's still not operational," said Paul Gauthier. Gauthier is vice-president, technical, with the Canadian Air Traffic Control Association, the union representing the country's controllers. "Government seems to be able to get themselves in the situation where they are paying through the nose and not getting the goods," he said.

The system has been in use at Calgary International Airport since June 6 and so far the system is working well, said Roger Westmore, Transport Canada's project manager. "There is a back-up, but we think it's unlikely it would be required," Westmore said.

That back-up is provided by controllers in Edmonton, and a switchover in the event of a major failure of the system would take five to 10 minutes, Gauthier said. "I couldn't believe it, but that's what they are doing," he said. "It's not certified or commissioned, but they are running live tests with live people." The massive program is known as the radar modernization project (RAMP) and is touted as one answer to easing congestion -- and reducing delays -- in the skies above congested airports, like Person International.

The new radar replaces vacuum-tube technology with a better picture of what's happening in the skies. That would allow them to space aircraft closer together and, in the end, get more flights in and out of busy Pearson.

Transport Canada officials say they are close to clearing "the last hurdle" and are optimistic that the system will be up and running at Pearson early next year -- 2 1/2 years after originally expected. The system should be fully operational across Canada within the next six months, Westmore said. But controllers and airline representatives are less hopeful. "That's the story we've been getting for the last three years. It's always just around the corner," said John Redmond, president of the controllers' association.

"It's crashed in Montreal. It's crashed in Moncton. It's crashed in Toronto," Redmond said. "The problem is primarily with the software not being able to handle the amount of data that runs through the system, and it keeps crashing," Redmond said.

Controllers who have experienced an unnerving system crash say they never know how long they'll be without radar when it happens. That's why the new system is losing the trust of the very people who will have to use it, Gauthier said.

The system screw-ups in testing include:

-- Switching the data tags between two aircraft when the planes are close together on the radar screen. The tags are vital, identifying the green blips on the screens.

-- Backing up targets on the screen, in essence showing jets flying backwards. Developing a software package that would work in Toronto Centre -- the busiest airspace in Canada -- has remained the big hurdle, sources say. One stumbling block has been the system's inability to handle heavy traffic. Just when designers think they have one glitch cured, another pops up, sources say. The curious problems struck as recently as last month, when the latest package of software was tested in Moncton and failed, they say.

Westmore denies the system failed and instead says it needed "additional improvements." With a project of this magnitude, it's normal to expect some problems, he said. The contract for the system was awarded to Raytheon Canada Ltd. in 1985.

### Fun with high pressure

Michael Stern <stern6@husc10.harvard.edu> 4 Aug 92 03:43:17 GMT

Beware of high pressure without passive safety devices! The following account of a near accident at a research university is constructed from conversations with a friend of mine who will remain nameless, as will his university.

Researchers were attempting to measure directly the permeability for melt transport through a matrix of partially molten rocks. This required the use of a digitally controlled high-pressure pump (a 25,000 psi Single-Cylinder Positive Displacement Pump manufactured by Ruska Instruments of Houston, TX.)

The pump was controlled by a ZEOS 386 clone via a serial line. On the day in question, the computer froze while the pump was compressing the system at full speed. Before dying, it sent enough garbage across the serial line to confuse the pump's keyboard, so that researchers lost all software control of the pump, which merrily continued to compress past the software pressure limit which had been set (corresponding to the maximum pressure for the tranducers in the system, 2000 psi). It got to 4000 psi, the threshold for permanent damage to the transducers, before they managed to switch the power to the pump's motor off. This is particularly scary because the pump will go to 25,000 psi, but the plumbing was rated only for 20,000 psi so it would probably have been an explosive failure.

They had had problems with the clone in the past; most of which were believed related to the Extended Memory Manager.

It should be noted that the following safety precautions would eliminate this type of danger: use of \_hardware\_ travel limit switch as well as software pressure limit. Also, any system with pressure-sensitive parts should always have at least one safety head equipped with a suitable rupture disk.

Michael Stern

#### Mr. C. Baggage, who was neither a Mister nor a Baggage at all

Geoff Kuenning <desint!geoff@uunet.UU.NET> Tue, 4 Aug 92 23:43:36 PDT

Some years ago, a cellist acquaintance landed a job on the opposite coast. Like all serious cellists, she bought a second ticket for her valuable instrument rather than subject it to the vagaries of airline baggage handling.

As it happened, someone near the destination later offered her the use of another fine cello so that she wouldn't have to bring her own. Stuck with an extra ticket, she successfully advertised it for sale. The only catch was that the purchaser had to identify himself as Mr. C. (for Cabin) Baggage when he boarded the flight.

It seems that the ticket-reservation system doesn't have a provision for tickets issued to non-persons. A blank field is an error, and there is no override. I've heard of some pretty creative names invented by cellists to identify their instruments on flights.

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

[She could buy a ticket for the 'cello case in the name of Justin Case -- just in case she needed the extra seat. Further confusions arise ticketing a baseball pitcher named Viola or someone associated with ClariNet. (Playing first bass/base is clearly ambiguous orally/aurally/AuraLee.) There are also rigorous orchestras with Horn Clauses in their contracts. PGN]

### ✓ Unreliable call-return phone feature...

Rex Black <rex@iqsc.com> Tue, 4 Aug 92 09:33:02 CDT

I know that caller ID has generated a number of discussions about privacy and risks to individuals. I'd like to pass on a personal experience I had with a related technology, call return.

I was using my modem and computer to telecommute on Sunday afternoon. Shortly after hanging up, my phone rang. The caller asked with whom she was speaking. I responded by asking who she was trying to reach. It turned out that she had just been the victim of a harassing phone call. Southwestern Bell has a phone feature (call return) that allows a person to press a star-sequence (i.e., \*1) to call back the last caller. According to the phone salesman who (aggressively) marketted it to me when I had my phone connected three months ago, it uses the same logic as caller ID. (He mentioned that Southwest Bell would offer caller ID in the fall.) He promoted call return as a "great way to deal with obscene or harassing callers." My experience Sunday afternoon points out a serious risk associated with such technology. Clearly, the system has a bug. That bug lead someone to believe that I was harassing them. Depending on what was said, the system identified me as a misdemeanant or a felon.

On Monday, I called Southwestern Bell and explained my concern. While the person I spoke with understood my concern, he did not help. He repeated the standard disclaimer about "no phone system is perfect, the phone company can not guarantee accuracy, blah, blah, CYA, CSWBA..." I did manage to get from him some further information: First, this was hardly the first time this happened. He mentioned that incidents like mine occur frequently. Second, the phone company's policy requires that, before turning a case over to the police,

someone must repeatedly call and harass someone. One instance does not suffice.

I then called the P.U.C. I spoke with a woman there who, when she realized I was calling to voice concerns about caller ID and call return, adopted a very tired tone of voice. She gave me a docket number and said that I should send in my comments to the P.U.C. I asked about groups who may have joined fight against such technology. She said that SWB had just submitted the caller ID request, but she expected that a number of people would get involved in the ensuing discussion. She did not sound pleased at the prospect.

Rex

### ✓ GTE's Personal Secretary

Chuck Ham <CMHAM01@UKCC.uky.edu> Tue, 04 Aug 92 08:20:27 EDT

General Telephone is just now offering the "Personal Secretary" voice message service to the public here. In recent newspaper ads GTE touts that the service takes messages, reminds you of important dates, has a wake up service, and can be programmed up to a year in advance. Sounds like I can throw away my answering machine, my date book, my alarm clock and my computer, all for the low price of \$5.95 a month with the first 30 days free!

Customers, however, are not made aware of some of the risks involved. A friend was recently made a victim of the service WITHOUT subscribing.

She noticed her home phone (which she always used to receive client calls) was not ringing and no messages were being left on her answering machine. Several times when she tried to dial out a strange tone came over the receiver. This went on for several days until her business associate complained of the same problems.

After discussing this with GTE my friend discovered that a church-friend that works for GTE signed up SEVERAL people without their knowledge. (She thought it was a "nice" thing to do.)

My friends problems with the "Personal Secretary" were caused by the way the system is set up. First, it answers on the first ring, therefore it wouldn't activate the answering machine or allow a person to answer. Second, without the proper code number you cannot retrieve your messages (the tone she heard was alerting her to the messages she had waiting... but of course she had no idea what it was for). Needless to say my friend was not impressed!

How could the phone company employee sign someone up without their knowledge or signature? Doesn't GTE have some legal obligation to notify a customer before tapping a service onto their line? Can they just do it without any proper authorization?

Chuck Ham chuck.ham@ukwang.uky.edu Radio/TV Information Specialist University of Kentucky

### 🗡 Police files

Nigel Allen <nigel.allen@canrem.com> Fri, 31 Jul 1992 20:00:00 -0400

New York Awarded Funds to Improve Criminal History Records To: State and City Desks Contact: Stu Smith of the Office of Justice Programs, U.S. Department of Justice, 202-307-0784 or 301-983-9354 (after hours)

WASHINGTON, July 30 /U.S. Newswire/ -- The U.S. Department of Justice has awarded the state of New York \$381,512 to continue its program of improving the quality of the state's criminal history recordkeeping, the Bureau of Justice Statistics (BJS) announced today. The project, administered by BJS in the Office of Justice Programs (OJP), is part of a three-year, \$27 million program established by the Attorney General to help states upgrade current systems used to maintain records of arrests, prosecutions, convictions and sentences. The Bureau of Justice Assistance is providing the funding through the Edward Byrne Memorial State and Local Law Enforcement Assistance Program.

"The major objective of this cooperative agreement is to improve the overall quality of the state's criminal history record information by improving disposition reporting, " said BJS Director Steven D. Dillingham. "This administration is making every effort to assure the highest standards of accuracy and timeliness in criminal history record information across the country. It is critical that law enforcement officers, prosecutors, judges and corrections officials have access to complete and accurate information on each individual within the purview of the criminal justice system," Dillingham commented.

The New York Division of Criminal Justice Services will use the assistance to correct database problems identified during the first phase of the program and complete a study to determine if problems related to disposition collection can be systematically resolved. "The program emphasizes the recording of arrest, conviction and sentencing information in a form that will make felony history information more reliable and complete," Dillingham commented. "This is a crucial component of the overall objective of insuring that state criminal history records are up-to-date and available to all criminal justice agencies." Additional information about this program is available from BJS. Publications and statistical and research data may be obtained from the National Criminal Justice Reference Service, Box 6000, Rockville, Md. 20850. The telephone number is 301-251-5500. The toll-free number is 800-732-3277.

Canada Remote Systems - Toronto, Ontario/Detroit, MI World's Largest PCBOARD System - 416-629-7000/629-7044

## Ke: User interface studies: oh, what's the use? (Slade, <u>RISKS-13.69</u>)

Steve Summit <scs@adam.mit.edu> Tue, 4 Aug 92 15:09:55 -0400

Robert Slade writes:

> Couple... at next ticket machine looking very

> worried...: "How do you work this?" Point out large legend at top... Point

> out large A by map, B by buttons, etc. Couple goes back to worrying in

> front of next ticket machine.

There's a fundamental problem here which we might as well lump together with computer literacy (or lack thereof). Many people have an instinctive, gut-level response to anything that "looks technical": "Oh, this is too complicated. I can never figure these things out." No amount of (impersonal) hand-holding in the form of allegedly idiot-proof instruction will help; these people's minds are firmly made up. ("The lady doth protest too much, methinks" applies -- if a technical system, for use by the masses, seems to need "idiot-proof" instructions, it's probably too late. Don Norman's POET discusses this phenomenon well, and at length.)

The instinctive response ("I can't figure this out") is irrational, because there are many allegedly idiot-proof technical systems out there which are truly inspired in the techniques they employ to achieve alleged idiot-proofness, techniques which render the interfaces accessible to just about anyone \*if they try\*. But remember, humans are basically irrational creatures (which only makes irrational responses harder to understand for those of us who occasionally try to be rational).

A lode that newspaper columnists have been gleefully mining lately is disgust (theirs and their readers') over voice mail systems ("push 1 if you would like to..."). These systems, when implemented well, can be much more efficient than waiting on infinite hold for harried, human operators. But the people doing the complaining want to talk to a person, they don't want to push buttons.

I think it will take a couple of generations before there is any kind of widespread approval and appreciation of these and other similarly technical systems.

Steve Summit scs@adam.mit.edu

### ✓ Sweet Old Things and User Interfaces (Slade, Re: <u>RISKS-13.69</u>)

Unix Guru-in-Training <elr%trintex@uunet.UU.NET> Tue, 4 Aug 1992 14:42:13 GMT

Robert Slade, in <u>RISKS 13.69</u>, describes the scene in front of various automatic teller machines and ticket machines and sees that in spite of clear and instructive diagrams (to him) people (especially older people) are still having trouble using automatic machines.

Although it's a little hard to read Robert's prose, he appears to be saying that no matter how smart the computer is, some people are still too stupid to use it. I'm a bit worried by that -- the readers of RISKS are all fairly sophisticated computer users who can handle the various commands of Unix, VMS and fourteen million different mail-readers. Have we forgotten that not everyone else in the world uses computers the way we do? That operating a machine, be it a soda vending machine, vacuum cleaner, bank machine, or Sun workstation, is not a skill human beings are born with? If the user interface is too difficult for most users to figure out, it's not the user's fault. It may not even be the machine's fault -- it may just be the job the machine is trying to do is too complicated for the average person. The problem is that is was designed by "computer geeks" like us, who don't have a problem learning a difficult interface.

Perhaps as the older generation passes, replaced by a generation born using Nintendos, remote controls, digital watches, and other accoutrements of the digitized era, the minimum ability of the average person to use a machine interface will increase. But until then, we shouldn't fall into the trap of blaming the victim for the inadequate user interface.

Ed Ravin elr@trintex.uucp elr%trintex@uunet.uu.net +1-914-993-4737

### re: Computer scoring glitch at Olympics (Carr, <u>RISKS-13.69</u>)

Stanley (S.T.H.) Chow <SCHOW@BNR.CA> 4 Aug 92 10:07:00 EDT

This is a good illustration of a problem that is often blamed on copmuter systems, particularly when cutting in a new system.

People forget that it is a different game.

The rules were changed (I presume at the insistance of the Americans as a result of the Soul Olympics), why should one expect the same result from the new rules as the old obsolete rules? The fact that a computer system was used to keep score under the new rules is neither here nor there (unless there has been a real computer glitch).

One can conjure up many different possible reaons why the new rules give a result different from the old rules, one can also argue endlessly as to which set of rules are better, but rules are rules.

To bring this back to RISKS: using a new computer system to implement a new set of rules can bring about surprising result, having people in the loop adds a degree of self-correction.

Stanley Chow (613) 763-2831

BNR, PO Box 3511 Stn C, Ottawa, Ontario, Canada K1Y 4H7 BitNet: schow@BNR.CA schow%BNR.CA.bitnet@relay.cs.net ..!uunet!bnrgate!bcarh185!schow

#### Ke: Computer scoring glitch at Olympics

Joe Konstan <konstan@elmer-fudd.cs.berkeley.edu> Mon, 3 Aug 92 19:02:55 PDT

In <u>RISKS-13.69</u>, John Carr presents a \_Boston Globe\_ except about a "computer glitch" that eliminated US boxer Eric Griffin. As someone who watched the

fight (tape delayed) on TV, and has been following the controversy, I'd like to add a few points that are missing from the article.

There are two main human reasons why the computer system, which most commentators thought functioned properly, would record such a score. First is the "Nintendo effect"--boxing judges don't tend to have particularly good reaction times, and therefore may miss the one-second cutoff. Second is a particularly bad judge, who recorded only 13 punches total while the others averaged 29.5. This judge had just returned from a two day suspension for poor performance.

To understand the system, it is somewhat useful to understand the layout of the ring judges. This picture is approximate:



Under the new scoring system, the main score is based on a majority of judges recognizing any punch. Since at least one, and often two will have obscured views, a single bad judge really can throw off the system WITHOUT ANY COMPUTER MALFUNCTION.

Finally, this particular match, while extremely shocking, is not that unusual. Throughout these olympics, a large number of clear punches, particularly to the body, have not been scored.

As we see again and again, a computer cannot take a poor system and make it better--but it can provide a focus for blame.

Joe Konstan

# Ke: computer scoring at olympics (<u>RISKS-13.69</u>)

David Wittenberg <dkw@cs.brandeis.edu> Wed, 5 Aug 92 19:08:41 -0700

If you don't know how to do something, you don't know how to do it with a computer.

The real problem is that boxing has not decided what they mean by "landing a blow". Note that the individual scores vary by more than a factor of 3. If the judges differ by a factor of three, how can they expect that software will mediate this difference? I suspect that the software did exactly what it was specified to do.

According to the commemtators, the new scoring system has changed the style of boxing. Computers cannot decide what the rules should be, but they can, and perhaps should, be used to see what results different rules

give, and one can they chose the rule that most closely correlates with the judges' impressions.

--David Wittenberg

### 1993 Symposium on Research in Security and Privacy

<kemm%cs@hub.ucsb.edu> Thu, 06 Aug 92 15:05:45 PDT

> CALL FOR PAPERS 1993 IEEE Symposium on Research in Security and Privacy Oakland, California, May 24-26, 1993

sponsored by IEEE Computer Society Technical Committee on Security and Privacy in cooperation with The International Association for Cryptologic Research (IACR)

The purpose of this symposium is to bring together researchers and developers who work on secure computer systems. The symposium will address advances in the theory, design, implementation, evaluation, and application of secure computer systems. Papers and panel session proposals are solicited in the following areas:

Secure Systems Privacy Issues Information Flow Network Security Formal Models Viruses and Worms Database Security Access Controls Security Verification Authentication Data Integrity Auditing and Intrusion Detection

#### **INSTRUCTIONS TO AUTHORS:**

Send six copies of your paper and/or panel session proposal to Richard Kemmerer, Program Co-Chair, at the address given below. Put names and affiliations of authors on a separate cover page only, as a ``blind'' refereeing process is used. Abstracts, electronic submissions, late submissions, and papers that cannot be published in the proceedings will not be accepted.

Papers must be received by November 15, 1992 and must not exceed 7500 words; papers that exceed this length will be rejected without review. Authors will be required to certify prior to December 25, 1992 that any and all necessary clearances for publication have been obtained. Authors will be notified of acceptance by February 1, 1993. Camera-ready copies are due not later than March 15, 1993.

The Symposium will also include informal poster sessions. Send one copy of your poster session paper to Teresa Lunt, at the address given below, by January 31, 1993. Electronic submission of the latex source for poster session papers is strongly encouraged. Poster session authors must send a certification with their submittal that any and all necessary clearances for

publication have been obtained.

**PROGRAM COMMITTEE** Tom Berson Paul Karger Jon Millen Anagram Laboratories OSF MITRE Deborah Cooper Jeff Picciotto Tanya Korelsky MITRE Paramax Systems Corporation ORA George Dinolt Sue Landauer **Phillip Porras** Loral Labs TIS Aerospace Virgil Gligor Teresa Lunt Ravi Sandhu University of Maryland SRI George Mason Univ. Deborah Hamilton Marv Schaefer Doug McIlroy Hewlett-Packard Laboratories AT\&T Bell Labs CTA John McLean Jeremy Jacob **Brian Snow** Oxford University NRL NSA Sushil Jajodia Catherine Meadows Yacov Yacobi NRL George Mason University Bellcore

For further information concerning the symposium, contact:

Teresa Lunt, General Chair	Cristi E. Garvey, Vice Chair
SRI International, EL245	TRW, MS R2-2104
333 Ravenswood Avenue	One Space Park
Menlo Park, CA 94025	Redondo Beach, CA 90278
Tel: (415)859-6106	Tel: (310)812-0566
FAX: (415)859-2844	FAX: (310)812-7147
lunt@csl.sri.com	

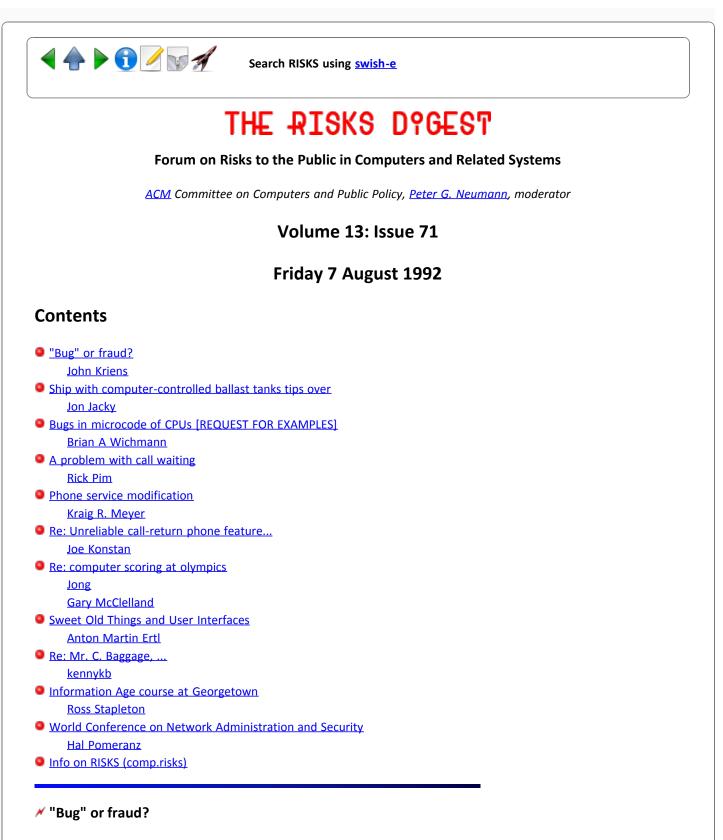
Richard Kemmerer, Program Co-ChairJohn Rushby, Program Co-ChairComputer Science DepartmentSRI International, EL254University of California333 Ravenswood AvenueSanta Barbara, CA 93106Menlo Park, CA 94025Tel: (805)893-4232Tel: (415)859-5456FAX: (805)893-8553FAX: (415)859-2844kemm@cs.ucsb.edurushby@csl.sri.com

Jeremy Jacob, European Contact Oxford Univ. Computing Laboratory 11 Keble Road Oxford, England OX1 3QD Tel: +44 865 272562 FAX: +44 865 273839 jeremy.jacob@prg.oxford.ac.uk



Search RISKS using swish-e

Report problems with the web pages to the maintainer



24474-kriens <decoy!jkriens@uunet.UU.NET> Fri, 7 Aug 92 14:12:46 GMT

The following appeared in the Thursday, Aug. 7, 1992, NJ Star Ledger.

"Bug" Backfires on Computer Consultant

NEW YORK (AP) -- A computer consultant must pay \$25,000 to a Manhattan law firm whose computer system crashed because he put a "bug" in it.

Donald R. Lewis hoped the bug would cause the law firm of Werner, Zaroff, Slotnick, Stern and Askenazy to call him for repair work after the system collapsed, according to Civil Court Judge Richard F. Braun. Lewis was hired in 1985 to upgrade the firm's computer system, which tracks medical payments of auto accident victims to health care providers. The patients, under the state's no-fault insurance law, assign their awards to the health care professionals. Lewis initially estimated the upgrade would cost up to \$5,000, but the firm eventually paid him some \$21,000.

In the months that followed, Lewis periodically called the firm's receptionist to see if the computer file had entered claim number 56789. In July 1986, six months after the firm made its last payment to Lewis, the computer system shut down. It had filed claim number 56789, Braun said. Lewis had put a "conditional statement" in the computer's software which caused it to stop functioning at claim number 56789, the judge said. The law firm paid another consultant \$7,000 to fix the problem.

[Once again this brings up the concern of people thinking that anything that happens in a computer system that wasn't expected by the end users is a bug. I'd like a job where I got paid \$7000 to remove a "conditional statement." John Kriens jkriens@decoy.cc.bellcore.com]

### Ship with computer-controlled ballast tanks tips over

Jon Jacky <JON@gaffer.radonc.washington.edu> Fri, 7 Aug 1992 9:15:48 -0700 (PDT)

From THE SEATTLE TIMES, Wed. Aug 5, 1992, p. D1:

"Ship makes list - the hard way" by Penelope M. Carrington

F. Garcia had just rounded the corner ... yesterday when he saw the 300-foot fish-processing ship list to its right and crash into the neighboring dry dock. ... the vessel, the Dona Karen Marie, had been leaning since early yesterday morning. First it listed to the left --- portside. Then an engineer came to fix the problem. Workers watched as the ... ship leveled and then listed to the right --- starboard --- into the United Marine Marketing dry dock.

Shipyard spokeswoman Ruth Nelson said something malfunctioned in the computer that controls the water-ballast tanks of the boat when the engineer tried to correct the original listing. As a result, all the water in the left tank "was swooshed down to the other side," said Nelson, who was unsure why the boat listed in the first place.

There were no injuries, and no danger of the ship tipping over into Lake Union because it rested against the firmly anchored dry dock.

Tacoma Boat, which built the Dona Karen Marie, was contacted to secure copies of the original plans to the ships ballasting system. The Seattle Fire Department hoped to find the pipes that would pump the water back to the port side. ... The Dona Karen Marie has been moored in the shipyard for weeks. Nelson said she could not identify the vessel's owner.

[I pass the scene every day on my way to and from work. It is quite a sight --- imagine a four-story building tipped over onto its neighbor. The ship is tipped about 30 degrees away from vertical, resting against the wall of the adjacent drydock. I don't know if it would have capsized if it hadn't struck the drydock, but it looks like it might have. It is lucky no one was hurt.]

- Jon Jacky, jon@radonc.washington.edu, University of Washington, Seattle

### Bugs in microcode of CPUs

Brian A Wichmann <baw@seg.npl.co.uk> Fri, 7 Aug 92 17:18:48 BST

I have a long, but unfortunately, confidential article about bugs reported to me in the microcode of microprocessors, including those used in `safety-critical' systems. I would like to collect further examples.

Clearly, such bugs could undermine safety-critical systems. I have a list of such bugs, but unfortunately, many are confidential. I should like to collect further examples. If I get enough non-confidential examples, I will post them to comp.risks.

Please send E-mail information to me and state whether your example should be kept confidential or not. Give full details, such as the microprocessor, date, and nature of bug. Thanks. Brian Wichmann, National Physical Laboratory (baw@seg.npl.co.uk)

# \* a problem with call waiting (prompted by recent related anecdotes)

Rick Pim <RICK@qucdnee.ee.queensu.ca> Fri, 7 Aug 1992 11:58 EST

Recently, a couple of entries attracted my attention: rex@iqsc.com (Rex Black) talked about "Unreliable call-return phone feature...", while CMHAM01@UKCC.uky.edu (Chuck Ham) mentioned problems associated with GTE's Personal Secretary (where a friend had troubles without even subscribing). I suspect that something like my small risk has been mentioned before, but who knows....

Last year, Bell Canada had a promotion in our area to flog (among other things) Call Waiting. It was mentioned in a glossy throwaway in our monthly bill that we were having Call Waiting installed on our lines (we have two) for a free trial period.

Shortly after this, I was at home and my S.O. [significant other] was out curling. The arrangement was that she would call me when she finished, I'd pick her up, and we'd go scare up something to eat. While waiting, I dialled in to work and probably read news. After a while I got occasional bursts of line noise but ignored them - the local phone lines are sometimes noisy. The

other phone never rang...

The other half of the story is that there was an increasingly grumpy person at the curling club trying to find me: calling home (I wasn't there, because, of course, the phone was ringing and not being answered), work, friends' places, and the like. It took a long time before she thought of using the other phone number.

The risk is small, but annoying: with the increasing use of phone lines for data, it is not necessarily the best decision to use a normal "ring" when a caller dials a busy line with call waiting on it. One should also read glossy throwaways more carefully. :-)

#### Phone service modification

### <kmeyer@aero.org> Fri, 07 Aug 92 13:30:48 PDT

About a year ago, I had my long distance service switched from MCI to AT&T without my authorization--and didn't find out until the bill came from my local phone company, Pacific Bell. I called AT&T who said they keep no record of where a switch request comes from (they insisted that I must have filled out a form, or that I told a telemarketer to switch me, etc). They did take down an incident report after I insisted on speaking to a supervisor's supervisor.

Pacific Bell told me that they do no verification if a long distance carrier requests a switch on a customer's phone line; they receive a tape with phone numbers on it and switch every number listed on the tape to AT&T. (Pacific Bell also wanted me to pay to switch back to MCI, which MCI ended up paying).

Kraig R. Meyer kmeyer@aero.org

[This gets us back to the problem of the meaning of "unauthorized access" where no authorization is required, or in this case the meaning of "authorized access" when no authorization is requested! PGN]

#### Ke: Unreliable call-return phone feature...

Joe Konstan <konstan@elmer-fudd.cs.berkeley.edu> Thu, 6 Aug 92 17:55:42 PDT

In <u>RISKS 13.70</u> Rex Black relates a story of being "called back" via RETURN CALL by a woman who believed he had made a harassing call.

This is yet another version of an old set of pranks that involve connecting together unsuspecting phone users. While most of us are more familiar with the version where a prankster with 3-way calling connects together two strangers (while listening in), I haven't heard much about people making harassing calls while having CALL FORWARDING activated to deflect the return call.

Unfortunately, until we can tell whether a call we make is being forwarded

(which may mean until we get ISDN, or the messiah comes, I'm not sure which is likely to come first), there is no way to prevent a prankster from deflecting calls to another line. Rest assured, though, that the switch does know who placed the call, and that CALL TRACE would properly finger the prankster no matter what forwarding was in place.

Joe Konstan konstan@cs.berkeley.edu

#### Re: computer scoring at olympics

Jong <jong@tnpubs.enet.dec.com> Thu, 6 Aug 92 19:17:25 PDT

I would like to think that a user-interface problem, not judging incompetence or favoritism, was the cause of the shocking loss by the US boxer.

In the third round of the fight, with the score tied at 2-2 (an obvious problem right there), the German threw a punch that missed, and the American landed a counterpunch that split the German's eyebrow open. The German was awarded a point!

How did this happen? Each judge has a box with two levers, one for each boxer. If the boxer in red lands a punch, the judge presses the left lever; if the boxer in blue lands a punch, the judge presses the right lever.

Now: The judges watch the fighters stalk each other, circle, and throw combinations. They press the left lever -- no, the right! Too late.

I think the judges all pressed the wrong lever.

### Re: computer scoring at olympics (<u>RISKS-13.69</u>)

Gary McClelland <mcclella@yertle.Colorado.EDU> Fri, 7 Aug 1992 10:26:46 -0600

Several RISKS contributors have correctly noted that the problem with the computerized scoring system used for Olympic boxing is not the computer but rather the button-pressing speed of the judges and the scoring rules that were implemented in the program. The computer RISK is that electronic implementation of complicated scoring systems, systems which would not be feasible without computers, allows scoring rules to be used whose consequences are not well understood. These new scoring systems often seem reasonable on paper but turn out to have surprising consequences. I'll bet boxing officials were surprised (embarrassed?) to learn that all judges could score a fight in favor of Boxer A but that the majority-rule-per-punch rule could give the decision to Boxer B.

The larger RISK is that implementations of "electronic town meetings" and telephone voting will allow the use of creative scoring systems for electing candidates and making policy decisions. Without extensive forethought, such computerized voting systems will inevitably produce unexpected results with more serious consequences than who receives boxing medals.

There need not be surprises. There is a large literature in the field of public choice on the formal analysis of voting and scoring rules. Kenneth Arrow won the Nobel Prize in Economics for, among other things, proving that if there are three or more options [not a problem for Olympic boxing] then it is impossible to have a scoring system without unpleasant surprises such as being manipulable and producing intransitive choices. Since then the search has been on for finding voting systems that have the fewest problems and a large array of analysis tools are available. The boxing officials ought to have consulted experts in the field of public choice as well as computer experts. Perhaps they did. The boxing rules may not be all that bad; they have a remarkable similarity to the rules NASA uses to resolve disagreements among on-board computers and NASA did consult with the public choice experts. However, in the boxing case, it is easy to show that conservative judges [these may not necessarily be the worst judges as alleged in the recent case] have a disproportionate impact because it is more likely that their votes will be decisive in forming the majority on any given punch. The punchline is that computers may allow us to get into kinds of political trouble with fancy scoring rules that would not have been possible with paper-and-pencil systems which are forced to be simple.

Gary McClelland Univ of Colorado mcclella@yertle.colorado.edu

#### Sweet Old Things and User Interfaces (Re: <u>RISKS-13.70</u>)

Anton Martin Ertl <anton@mips.complang.tuwien.ac.at> Fri, 7 Aug 92 16:27:27 +0200

Ed Ravin (elr%trintex@uunet.uu.net) and Steve Summit (scs@adam.mit.edu) hope that the next generations will have less problems with (the user interfaces of) machines due to childhood training at Nintendos etc.

I doubt this: I notice that I become more impatient the older I get. I spent countless hours learning the tricks of my programmable calculator. Nowadays I am too impatient to read the manual of my video recorder. When in ten years they force me to use ATMs, I will probably even be too impatient for learning that, especially if there are people waiting in the line (and it does not matter that learning the system is the fastest way to get it done). As an analogy, we have had forms since the invention of bureaucracy, but they still confuse us.

M. Anton Ertl anton@mips.complang.tuwien.ac.at

### Ke: Mr. C. Baggage, ... (Geoff Kuenning)

<kennykb@dssv01.crd.ge.com> Fri, 07 Aug 92 10:16:23 -0400

In <u>RISKS-13.70</u>, Geoff Kuenning tells the story of a Mr. Cabin Baggage (actually a violoncello) having a ticket on an airline flight. Having to ticket cabin baggage that way is a potential RISK to a search and rescue party in the event that the airplane crashes, since if the ticket is used, the passenger list will

show one more soul on board, and the rescuers will be looking for another potential survivor. It would be a tragedy if a rescuer someday lost his life trying to find Mr. Stradivarius Cello.

I know that I've had cabin baggage successfully ticketed by United without having to come up with a fictitious name; some reservation systems do it right.

But musicians seem to get into this type of trouble. The duo-pianists Stecher and Horowitz once arrived at the airport to find that the rear row of seats had been removed from the aircraft to accommodate the stretcher -- they'd been booked as `Stretcher patient, Horowitz!'

[When dealing with computerized systems, we must be forewarned that we need to be forearmed. But for pianists, four-armed can be four-handed on one keyboard or duo-piano, on two. But the absence of seats cannot be forewarmed. PGN]

[Incidentally, since I am already drifting in relevance (too much flying?), John Levine (johnl@iecc.cambridge.ma.us) noted that a professional cellist friend of his regularly buys a seat for his cello, but the airlines won't let the cello join a frequent flyer program. It would probably do violins to their computer system. At any rate, this is certainly enough for this topic... Thanks for your indolcence. PGN]

#### Information Age course at Georgetown

### <"stapleton@misvax.mis.arizona.edu"@Arizona.edu> Thu, 6 Aug 1992 15:33 MST

For those in the greater Washington DC area, I will be teaching a course in Georgetown University's continuing education program, surveying issues arising from our entry into the "Information Age." The course description is below, and it runs for eight Thursday evenings. Contact the School of Summer and Continuing Education at Georgetown for further information (and forward this note to others if you like). Ross

#### 

#### ISSUES FOR THE INFORMATION AGE

This course will address issues of the "Information Age" for a nontechnical audience, i.e., how computers and computer-based information and systems are transforming the world around us.

What does it mean to say that "information about money is as valuable as money itself?" Many companies do nothing more than broker information, as an increasingly larger percentage of the U.S. economy. But where ought the boundary between commercial profit and personal privacy be drawn? Lotus Development Corp. cancelled its plans to market a database on consumers in the face of protests from those it would have monitored, and across the U.S. "caller ID" technology is facing severe scrutiny from all sides.

In the wake of the failed Soviet coup, a U.S. communications company took out a full-page ad to congratulate Soviet citizens who, "armed with nothing more than information...saved the day." News of the Tiananmen Square massacre came to us out of China by way of portable satellite dishes and the fax machine.

Information systems are making life more efficient, but never before has it been possible for a simple computer glitch to cause a billion dollars worth of damage--twice in 1991 software bugs crippled large portions of the U.S. telephone system, and a Cornell graduate student's program shut down tens of thousands of networked computers in 1988. [WELL, Cliff Stoll estimated 2,600 of the estimated 6,000 BSD Unix systems. PGN]

The legal profession is scrambling to apply yesterday's laws to new realities, and "artificial reality" has been used in court testimony, while the FBI lobbies to make digital telephones easier to wiretap. What do we have to fear from "hackers?" Does computer crime pay?

Readings will be provided, taken largely from the current press, to serve as background and focus for discussion.

Dr. Ross Alan Stapleton is a science and technology analyst with extensive experience studying computer and information technologies in the former USSR and Eastern Europe.

8 sessions, Thursday evenings, 7:45 to 9:15 p.m., September 24 through November 12, 1992.

# World Conference on Network Administration and Security

Hal Pomeranz <pomeranz@nas.nasa.gov> Thu, 6 Aug 1992 12:59:17 -0700

> CALL FOR PAPERS AND PRE-ANNOUNCEMENT The 1992 World Conference On Network Administration and Security November 30 - December 4, 1992 Washington, DC

THEME: Practical solutions for cost-effective network administration and security in a UNIX environment.

ELIGIBILITY: Network administrators, system administrators, security administrators, technology managers, computer installation managers, and their staff. In addition, a limited number of places are available for staff members from organizations that offer off-the-shelf software and hardware products that support network management and security.

LOCATION: Ramada Renaissance Techworld Hotel, 919 9th Street NW, Washington, D.C. 20019, (202) 898-9000

CONFERENCE DATES: Tutorials: November 30- December 1 Technical Sessions: December 2- December 4

INFORMATION: For pre-registration materials, send mail to:

Program Chairman, Alan Paller, Conference Office, 4610 Tournay Road Bethesda, MD 20816 or send email to paller@fedunix.org.

HOST ORGANIZATION: The Washington Area UNIX Users Group and the Federal Network Administration Council.

CONFERENCE SPONSOR: the Open Systems Conference Board, a not-for-profit educational organization dedicated to removing the barriers to widespread adoption of UNIX and Open Systems.

WHY YOU SHOULD PARTICIPATE: The demands of mission critical applications are driving the need for network innovation at an amazing pace. New technology and new standards promote confusion and interoperability problems while at the same time providing much needed connectivity and increased bandwidth. Cutbacks have forced fewer people to provide more service with less money.

These challenges are particularly apparent and frustrating in the government agencies (both in the US and abroad), universities, and companies which have been in the vanguard of the move to open systems and networks of UNIX computers.

This conference is designed to identify the current state of the art for cost-effective network administration and security so that the techniques and tools used by the most effective managers can be adopted by those still looking for solutions.

Peer-reviewed papers will be complemented with invited papers plus

"Ask the Experts" sessions where you'll find practical answers to your questions.

"Best Of The Net" session where you'll learn which free programs available from the net are most useful.

"Tips and Techniques" sessions in which conference attendees can share, in 5-minute presentations, their favorite techniques for solving recurring problems. These sessions are run as moderated BOFs with all conference attendees being asked, in advance, to contribute if they choose.

"Ask OSF" session where you can learn from the people who brought you DCE.

Informal Birds Of A Feather sessions in the evening to expand the sharing time. Please send your suggestions for topics with your registration.

In addition, the Monday-Tuesday tutorials will be taught by several of America's top-rated instructors. Tutorial topics include TCP/IP and UNIX Network Programming, UNIX Security, OSF DCE and DME, UNIX Fundamentals, UNIX Internals, UNIX System and Network Administration (Basic and Advanced courses), and Perl Programming.

\*\*\*\*\*

\*\* CALL FOR PAPERS \*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Papers are being sought for the technical conference from network administrators, system administrators, security managers, consultants, academics, and hardware and software developers.

You don't have to have made a major breakthrough to have your paper accepted. The delegates will be looking for good problem definitions and practical solutions. And your presentation does not have to be long. You may choose a 15, 30, or 45 minute time slot.

IMPORTANT DATES FOR SUBMISSION:

Abstracts Due: September 14, 1992 Notification of Acceptance: October 12, 1992 Camera-Ready Papers Due: November 16, 1992

FORMAL REVIEW: Papers that have been formally reviewed and accepted will be presented during the conference and will be published in the conference proceedings. The Review Committee is composed of experts on network administration and security along with managers of large installations and architects from the vendor community.

Among the people invited to serve on the Review Committee are Matt Bishop (Dartmouth), Michele Crabb (NASA Ames Research Center), Richard Stevens (author of several best selling books on Network and UNIX Programming), Marcus Ranum (Digital Equipment Corporation), Jonathan Gossels (OSF), and Bruce Hunter and Rob Kolstad (well-known columnists).

The committee will decide whether your abstract addresses important challenges (large or small), whether your approach seems promising, or whether your abstract should be accepted for any other reason.

TOPICS: Please feel free to submit abstracts on any topic. The list provided below may help prompt some ideas:

- 1. Managing heterogeneous networks
- 2. Policies and procedures on the network
- 3. Security policies
- 4. Network security monitoring
- 5. Network monitoring and performance testing
- 6. Training and education
- 7. Techniques for dealing with users
- 8. Networked backup schemes
- 9. Distributed mail systems
- 10. Domain Name Service configuration
- 11. Distributed console access
- 12. OSF's DCE and DME
- 13. Off-the-shelf tools
- 14. Tools you don't like and why

ABSTRACTS: A good abstract will by 500 to 1,500 words in length and

include the following:

- 1. A description of the problem(s) and its importance.
- 2. Your solution including details of how it worked. If this is work on emerging technology, try to show what the expected impact will be. If your solution is based on commercial hardware or software tools, name them. Abstracts from vendors are welcome, but should not be sales pitches.
- 3. Data on how well it works: before/after comparisons, direct savings, trade-offs, etc.
- 4. Lessons learned and what you might have done differently.

Please also provide the following information about the author(s): name, title, organization, daytime telephone, surface mail address, email address (please), FAX if possible.

Finally, tell whether you want a 15, 30 or 45 minute time slot for your presentation.

WHERE TO SEND YOUR ABSTRACTS: Technical Program Chairman Hal Pomeranz NASA Ames Research Center M/S 258-6 Moffett Field, CA 94035-1000

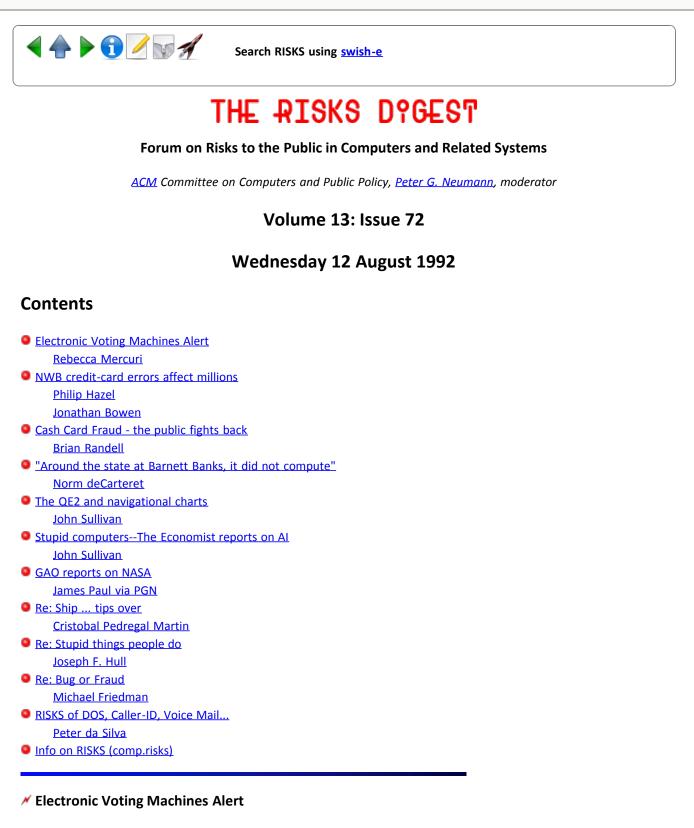
Questions or abstracts (PostScript or ASCII) may be submitted via email to pomeranz@nas.nasa.gov.

[Because many of our risks involve networking, it seems appropriate to include this item. On the other hand, as RISKS readers, you should be prepared to ask lots of nasty questions if you attend. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Rebecca Mercuri <mercuri@grad1.cis.upenn.edu> Wed, 12 Aug 92 04:16:11 EDT

On July 23, 1992, New York City Mayor Dinkins announced in a press conference that the \$60,000,000 contract to replace the city's mechanical voting machines with electronic voting systems (EVM) would be awarded to Sequoia Pacific, pending the outcome of public hearings.

The city's press release included the following statement: "In January 1989, SRI determined that Sequoia Pacific was best positioned and most willing to modify its system to meet the needs of New York City and New York State standards."

In actuality, SRI's Final Report (Evaluation of Offerors for the Procurement of an Electronic Voting System, December 23, 1988) contained the following first sentences under FINDINGS:

"No offeror's system completely meets the RFP specifications. On the basis of our analysis and the testing of the EVMs, SRI concludes that no offeror currently has either an EVM or central system acceptable for the city."

#### They went on to say:

"No offeror scored higher than 63% of the total possible RFP and evaluation criteria points."

#### And:

"SRI does not believe any of the four offerors has fully met the requirements of the RFP, based on their proposed EVMs, their central systems, and/or management and financial considerations. Each offeror would have to make substantial, significant modifications and additions -- in both technical and management areas -- for its approach to be considered acceptable for the City."

SRI went on to recommend Sequoia on the basis that of the four offerors, they had the greatest "probability of ... successfully implementing an electronic voting system for New York City."

Does the record indicate that Sequoia has or can successfully implement a system for New York City? You decide. Here is some information from public documents:

#### Monroe County, Indiana vs. Sequoia Pacific:

"In December, 1988, Monroe County, Indiana, filed a lawsuit against A. E. Boyce and SP, alleging that the defendants breached a contract between the County and Boyce whereby Sequoia was to have manufactured and Boyce was to have delivered to the County 120 automatic voting machines. Only 40 of the machines were delivered and Sequoia subsequently ceased production of the model which was the subject of the contract." "In December, 1990, the case was settled by the parties. The contract in question was terminated..."

On July 11, 1990 the Sequoia Pacific Electronic Voting System was denied certification in the state of Pennsylvania on the following grounds:

"(1) The system does not conform to Pennsylvania statutory requirements for overriding straight-party votes in individual offices; (2) the system can be placed inadvertently in a mode in which the voter is unable to vote for certain candidates, which is volative of statute; and (3) the system reports straightparty votes in a bizarre and inconsistent manner."

The NY City Board of Elections stated in a letter on January 3, 1991 that:

"The vendor has admitted to us that release 2.04 of their software used in the Pennsylvania certification process had just been modified and that it was a mistake to have used it even in a certification demonstration."

In what appears to be the final updated evaluation by SRI (June 19, 1991) of the Sequoia Pacific EVM and its Programmable Memory Device (PMD) which contains the vote tally, under the heading of Reliability, the testing status report from Sequoia Pacific stated:

"SP doesn't know how to show that EVM/PMD meets requirement -this depends on poll workers' competence."

If the above concerns you, here's what you can do:

 Attend and comment at the public hearings in New York City. It is critical that individuals have their opinions on this matter stated for the record, BEFORE the contracts are presented for signing. New York City residents as well as ALL other interested parties are permitted to attend. The meetings are: August 20, 42nd & Broadway, 6th Floor, 6PM September 10, City Hall, 10AM (tentative)

2. Request documents from the city under the Freedom of Information Act. Contact Lorraine Jones at 212/566-3307 in the Department of General Services. You may wish to request all or some of the following:

A. SRI Final Report, Volume I, December 23, 1988, Evaluation of Offerors for the Procurement of an Electronic Voting System.

B. SRI Updated Evaluation of the Sequoia Pacific EVM, June 19, 1991.

- C. Technical Specifications including -System Requirements Documents System Design Documents System Quality Documents System Verification Plan System Test Plan Results of Entire System Test
- D. A list of other publications relevant to this matter.
- 3. Write letters of concern and comment to:

Daniel DeFrancesco Executive Director Board of Elections City of New York General Office, 32 Broadway New York, NY 10004

cc separate copy to Stephanie Dawson Director, NYC Elections Project at the address above Kenneth Knuckles Commissioner Department of General Services Municipal Building, 17th Floor New York, NY 10007

cc all correspondence to Election Watch P.O. Box 1166 Philadelphia, PA 19105

- 4. If you are a member of ACM, IEEE or other professional, computing or engineering organizations, encourage your officers and club members to become involved and informed on this issue.
- 5. Forward this posting to everyone you believe would be interested in commenting on this matter.

Rebecca Mercuri mercuri@gradient.cis.upenn.edu

# NWB credit-card errors affect millions

Philip Hazel <ph10@cus.cam.ac.uk> Wed, 12 Aug 92 10:09:31 BST

Is there a record for the greatest number of people affected by one computer bug? [This is most likely not it. But it also depends on how you define "affected"... PGN]

BANK WARNS CREDIT CARD CUSTOMERS [Cambridge Evening News, 11 Aug 1992]

Millions of credit card customers are being contacted to be told their statements might be wrong. NatWest [the National Westminster Bank] is to tell its five million cardholders about the possibility of errors caused by a computer problem - and millions of cardholders with other banks who also have their accounts processed through the same system could be affected. But no-one will lose money as a result of the errors, said a NatWest spokesman. [No-one? Not even the banks? You bet, not the banks...]

The mistakes have come about because of a "blip" in the computer system run by First Data Resources. Cards affected include Visa, Mastercard and Access supplied by NatWest, Midland and Lloyds. `We will be correcting it all ourselves. There will be no need for the customer to contact us', said a bank spokesman.

[This item was also reported on ITN's TV newscast, where they interviewed a customer whose statement had spuriously acquired a debit for over 4,000 pounds. The credit card bill had automatically been paid from his regular bank account by Direct Debit, thereby making the bank acount overdrawn and attracting heavy interest charges.]

University Computing Service, Computer Laboratory, Pembroke St, Cambridge CB2 3QG, England P.Hazel@ucs.cam.ac.uk JANET: P.Hazel@uk.ac.cam.ucs +44 223 334714

# Mugs and bytes bedevil those paying by plastic (Re: Hazel)

<Jonathan.Bowen@prg.ox.ac.uk> Wed, 12 Aug 92 14:47:43 BST

> [... Jonathan sent in a bunch of further stuff on this topic, excised for brevity. PGN]

Last night's ITN 10 o'clock news was rather more sensationalist, showing a short clip of someone on the phone complaining about an unexplained debit of over 4000 pounds sterling (c \$7,500) entry on his account. Surely this must have been a set-up!

Jonathan Bowen, Oxford University, a Midland VISA card owner.

[In addition, lake@rcwcl1.dnet.bp.com sent in a copy of a U.S. State Department advisory along similar lines. PGN]

# Cash Card Fraud - the public fights back

# <Brian.Randell@newcastle.ac.uk> Wed, 12 Aug 1992 10:50:42 +0100

The following is the latest in a series of articles that I have seen in various papers over the last few months about a growing campaign against the practice that UK Banks have of assuming that all cash card fraud is due to stolen or misused cards and pin numbers. (This continues despite the case of the proven cash card fraud carried out by an engineer working for the Clydesdale Bank, if I remember correctly, who eavesdropped electronically on cash dispensing machines.) As I understand it, class actions are comparatively rare and difficult in the UK, so the story is locally interesting just for that reason. However I have not before seen any mention of the way that the barrister leading the action has arranged for computer database and communications technology to be used to gather evidence to counteract the banks' claims - hence this posting to RISKs. Brian Randell

-----

Banks face legal challenge over cash card fraud By Susan Watts, Technology Correspondent, The Independent, 12 Aug 1992

People convinced they have lost money through cash dispenser fraud could have a novel computer system to thank if they succeed in legal action against their banks due to start tomorrow.

Alistair Kelman, a barrister acting for aggrieved customers in a case against seven high street banks and building societies is using computer software to spot patterns in the way unauthorised transactions take place. Mr Kelman has built up a computer database holding information on more than 400 cases. His "relational" database allows him to cross-correlate the place, date and time of mystery cash withdrawals. He hopes to match cases with similar characteristics in a way that he says the banks have so far failed to do. The database will let him analyse "the spider's web" of automatic teller machines across Britain, he said.

"I don't think the banks are capable of doing what we are doing. They would only have the pattern of their own branch or their own banking network." Rebecca Evans, a barrister working for the Consumers' Association, said she had already noticed that victims often lived in the same area. Banks have also claimed phantom withdrawals occur near the victims' local cash machine, implying that their personal identification number has been passed on or stolen. She said the database should help to support or dispel such theories.

Mr Kelman believes the case is unusual in that it enlisted help from thousands of interested observers via a computer "conference" on the Compulink Information Exchange. This type of electronic message service lets people add their ideas to computer-based "conversations" via telephone data links.

Mr Kelman said the case had attracted about 5,000 contributors including policemen, people offering advice on how to make phantom cash withdrawals and others who had had first-hand experience of cashcard theft. One story added to the computer bulletin board recently was from a man claiming his high street bank account was debited from Scotland while he was sitting an exam in Chester with the card on his desk as proof of identification. The bank involved paid up almost immediately, despite the banks' persistent claim that their machines are infallible.

Mr Kelman said that linking the cases via his database has enabled him to bring a "group action" against the financial institutions.

Denis Whalley, associate solicitor at Keith J Park in Merseyside who is preparing the cases, said Mr Kelman's approach had helped him secure legal aid for many of the plaintiffs even though most were claiming less than (pounds)1,000, which would normally be too small a claim to qualify. He intends to issue writs on 10 cases tomorrow, then add to these over the following months to work towards a full trial next summer.

Mr Whalley said the banks had become more willing to pay up as his court case approached. But a spokesman for the Association of Payment Clearing Services the banks' cheque clearing system insisted yesterday that the banks were confident in the security of their computer systems and fully prepared to face the court action.

Dept. of Computing Science, The University, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

# "Around the state at Barnett Banks, it did not compute"

Norm deCarteret 813-878-3994 (TL 438) <normdec@vnet.ibm.com> Wed, 12 Aug 92 08:50:50 EDT Source: St Pete Times, 8/12/92, pg E1, Robert Trigaux

By the close of business Tuesday, Barnett Banks Inc had learned what it is like to be an 800-pound gorilla wearing a blindfold. Florida's largest banking company opened its 550 branches statewide Tuesday only to find its computers were taking the day off...branches could not open a new account or check balances in any customer's account.

Most branches set dollar limits on cashing checks and worked to minimize the confusion. But Barnett customers with big transactions to make and who did not pass a 'Do I know you' test of branch managers were out of luck for the day. ...

Though computer experts spent most of Tuesday in search of the 'bug' that plagued Barnett's systems, they were not able to identify it and fix it before most of the bank's offices closed at 4 PM. As it turned out, a single transaction ground Barnett's two giant mainframe computers to a halt, according to Jonathan Palmer, Barnett's chief technology officer.

"A coding error in a program caused our whole computer complex to 'hang up' ... That one transaction acted like a computer virus" by redirecting the computers from their appointed tasks. Barnett is working on new systems to avoid any repeat of Tuesday's troubles. "This should be an extremely rare occurrence," Palmer said.

A more detailed description of how the bug "redirected" their
computers and in such a way that the offending transaction couldn't
itself be located or help find the bug during the whole day would
be interesting. Other risks naturally include being a bank user
who customarily uses ATMs or uses different branches for convenience.

Norm deCarteret

IBM Information Network Tampa FL

# M The QE2 and navigational charts

<sullivan@geom.umn.edu> Wed, 12 Aug 92 11:34:11 CDT

The ocean liner QE2 had its hull damaged sailing near Martha's Vineyard. Nautical charts of the area (made in 1939) show a shoal at a depth of 39 feet (surrounded by readings of 85 and 90 feet) near where the ship hit something. The ship's draw is listed as 32 feet, which should have left seven feet to spare. (Of course, it is not known if this is what was hit, or if the pilot, a local pilot brought on board to navigate coastal waters, would have tried to stay clear of that ledge even if there was supposed to be seven feet clearance.) The entire area has been known as a dangerous one for ships for centuries, though the QE2 was in a standard navigation channel, heading for NYC.

An article in the NY Times today (12 Aug) points out that the nautical charts are based on a "sonar technology that may have overlooked higher peaks or boulders on an underwater ledge", described by an NOAA spokesman as "hit or miss". He said "It is possible that the survey missed a shallower depth, that the survey passed around it and didn't see it."

It surprises me that surveyors, when finding a steep shoal like this, 50 feet higher than the surroundings, would not look specially for its tip. This points out the danger of digitizing real world data onto a fixed grid.

Today's article in the Times (by Felicity Barringer) ends by noting that "at least two of the ship's three electronic navigational systems were operating at the time" of the accident.

-John Sullivan@geom.umn.edu

#### Stupid computers--The Economist reports on AI

<sullivan@geom.umn.edu> Mon, 10 Aug 92 14:03:24 CDT

The Aug 1st issue of the Economist has an editorial and article on "Stupid Computers". They say attempting to pass the Turing test is a bad idea, because computers think differently than people. Computers and people can complement each other. American Express, having computerized its credit card division, can now hire humans who are good at dealing with people (instead of at number crunching), and can give them more freedom to solve customers' problems (with the computer's help).

The article starts out:

Every customer has at least one horror story to tell of a company or a government deptartment that is unable to stop sending wrong bills, or to correct an address, or to divulge a piece of information "because of the computer". Teh brainless obstinacy of some machines has made them great allies of bureaucratic solution blockers. So the very thought of giving machines more responsibilities will send chills down many spines. Fear not. Companies are findin that the more intelligent machines are allowed to play to their strengths. the more they reduce human obstinacy.

However, it does conclude on a note of fear:

Someday someone will inevitably go too far. Bankers, for example, are talking about using artificial intelligence to enable their people to sell financial products too varied and sophisticated for the salesmen to understand. Now that is an intelligent idea that could leave someone looking very stupid indeed.

I don't see qualitative difference between this scheme and the one that allows American Express to hire people who don't understand the number crunching.

-John Sullivan@geom.umn.edu

✓ GAO reports on NASA, the latest from James Paul, paul@nova.house.gov

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 11 Aug 92 10:36:07 PDT

\* Space Station: NASA's Software Development Approach Increases Safety [Risks] and Cost Risks. US Government Accounting Office. Report to the Chairman, Committee on Science, Space, and Technology, [U.S.] House of Representatives, GAO/IMTEC-92-39. June 1992.

[The above title was DISAMBIGUATED by the insertion of "[Risks]" by PGN. The first time I read the title, it seemed to suggest that the approach increases safety. The text clearly indicates that is NOT what was meant.]

\* Space Shuttle: NASA Should Implement Independent Oversight of Software Development. US Government Accounting Office. Report to the Chairman, Committee on Science, Space, and Technology, [U.S.] House of Representatives, GAO/IMTEC-91-20. February 1991.

Copies may be obtained directly from the GAO (P.O. Box 6015, Gaithersburg MD 20877), or through James Paul (paul@nova.house.gov -- if his system is up!). These are relatively incisive and useful reports. Thanks, James! PGN

# Ke: Ship ... tips over (Jacky, <u>RISKS 13.71</u>)

<pedregal@cs.umass.edu> Fri, 7 Aug 92 21:12:28 EDT

[Jon Jacky reproduces \_Seattle Times\_ item on a ship that leaned left then right, the article then says:]

> Tacoma Boat, which built the Dona Karen Marie, [...]

"Tacoma" seems to have something with to do with bad oscillations :-)

Cristobal Pedregal Martin, Computer Science Department, UMass/Amherst MA 01003

[It certainly Narrows ones thinking! PGN]

# Re: Stupid things people do

Joseph F. Hull <jhull@muse.den.mmc.com> Tue, 11 Aug 92 14:56:31 MDT

I was working as a programmer for a military command center, the kind with large screens around the walls which display current status of whatever. The system was a custom job with custom software, but was fairly stable (no outstanding software problem reports, no recent modifications). Normal operations 24 hours / day, 7 days / week.

One Monday morning about 0600, the system crashed. No problem. The operator initiated warm start on the hot backup system and dump procedures on the failed machine; back on-line in less than 3 minutes (and called me, midnight shift

programming support). A few minutes later the alternate system crashed. What to do? (The dump takes about 11 minutes. If we abort the dump to get on-line as fast as possible, we lose any chance of finding out why the first crash occurred. And the primary system may go down again if we have an unrepaired hardware problem. But since both systems crashed within minutes of each other, its probably a software problem, so if I don't get the dump, we have ZERO chance of finding out what happened.) Call the command post for permission to complete the dump. Denied. Abort the dump. Reboot the primary. Initiate dump on the alternate. The primary crashes again. Reboot the alternate. Initiate dump on the primary. The alternate crashes again. This time we get permission to allow the dumps to complete. Reboot and back on-line. By now, it's after 0700.

Start analyzing what happened. Trace the problem to a data input routine. Hmmmm. Seems like its overrunning the buffer and trashing an adjacent data structure. Can't be, the buffer is already larger than the physical limit on the terminal (an IBM 2701 - a then modern but now ancient IBM Selectric ball-type typewriter rigged as a computer input device). Quick fix: move the adjacent data structure further away from the buffer, re-assemble (Yes, Virginia, we had computers before we had compilers. What's that, you little snot? Yes, I did work on them and no it was not before Christ.), bring the alternate to "hot backup" status and do a switchover. Take a deep breath and start figuring out WHY it happened, because the General has missed his Monday morning briefing and is going to want to know whether he cna count on his primary command and control system or not.

Hit a stone wall. Couldn't find anything wrong with the code. So I put an alarm in that input routine, took my chewing out and went on with life. Two weeks later, my alarm went off. The system didn't crash because I had moved that fragile data structure, but it would have if I hadn't moved it. The alarm also triggered an on-line dump and, when I checked it, sure enough, that same terminal had overrun its buffer again. But it can't! The buffer is 128 characters deep and the IBM 2701 is only 85 characters wide; you HAVE to enter a carriage return to continue.

Well, not quite. I finally made the connection between one particular Major inputting data for the General's morning briefing and the alarms. It seems this Major had figured out that the display screens could handle lines 132 characters long even though the input devices could only provide 85. So when he got to the end of a line on the terminal, he would grab the typewriter ball, drag it to the left, manually roll the paper forward and keep typing. As long as he was entering less than 128 characters, everything was ok. But when he went over that, ...

OBSERVATION 1: A user will do anything (s)he can think of to get the job done. OBSERVATION 2: They are usually more creative than we are, i.e., they think of things we don't.

Jeff Hull, 1544 S. Vaughn Cir, Aurora, CO 80012 303-977-1061 hull@den.mmc.com

Ke: Bug or Fraud (Kriens, <u>RISKS-13.71</u>)

Michael Friedman <mfriedma@us.oracle.com> Sat, 8 Aug 92 23:27:44 GMT

Lewis had put a "conditional statement" in the computer's software
 which caused it to stop functioning at claim number 56789, the judge
 said. The law firm paid another consultant \$7,000 to fix the problem.

- > [Once again this brings up the concern of people thinking that anything that
- > happens in a computer system that wasn't expected by the end users is a bug.
- > I'd like a job where I got paid \$7000 to remove a "conditional statement."
- > John Kriens jkriens@decoy.cc.bellcore.com]

I all fairness, let's note that the new consultant was probably expected to vet the code for any more unexpected surprises. Personally, I think \$7,000 was pretty cheap considering all the ways you can hide a whammy in code.

#### RISKS of DOS, Caller-ID, Voice Mail...

Peter da Silva <peter@taronga.com> Tue, 11 Aug 1992 14:09:17 GMT

Under (price) pressure, failures certainly become more common:

>Beware of high pressure without passive safety devices!

This is the same problem as our perrenial fly-by-wire discussion, so I'll let that part of the message stand. I would like, however, to raise another point:

>The pump was controlled by a ZEOS 386 clone via a serial line. [...]

>They had had problems with the clone in the past; most of which were believed >related to the Extended Memory Manager.

Ah. Doing real-time control under DOS or Windows. I couldn't imagine speccing a DOS based system for real-time control where system failure could lead to physical harm. I'm even leary of the use of an AT bus based machine: given the cost of the rest of the system and the risks involved I'd suggest buying a professional quality real-time control system rather than using this sort of hobbyist equipment.

Yes, we use DOS systems as part of real-time control systems, but only for man-machine interface (monitoring, supervisory control, and so on). And we typically buy the PC from one of the vendors that sells industrial quality equipment. Yes, a 19-inch rack-mount passive-backplane box may cost several times as much as a generic clone, but it's worth it.

If you MUST use a PC, there are real-time systems available: QNX, LynxOS, iRMX, and so on. iRMX even comes with a Windows-capable compatibility box, so you can run your DOS and Windows software... though I'd strongly recommend against it, at least while the experiment is under way.

(note that this is not a panacea: the (presumably professionally implemented)

real-time control system in the pump itself apparently failed as well... but at least it does give you a fighting chance at producing a reliable system)

#### ===

On another note, I'm concerned about the possibility of "frequent" mistakes in Southwestern Bell's Caller-ID system. I'm strongly in favor of Caller-ID as a concept, and have said so here and in TELECOM digest in the past. I did, however, assume that it would be approximately as reliable as the rest of the phone system: wrong numbers that are not the result of misdialing are quite rare. If there's a problem in Call-Return shared by Caller-ID (which is possible though not obvious: the dialler at the CO that Call-Return uses might be at fault) then I would certainly want it fixed BEFORE it goes on line. I'd even support pulling Call-Return until the problem can be resolved.

Pat Townson of TELECOM Digest has apparently seen no signs of this up in Chicago, so it may be a local problem. Southwestern Bell has not impressed me with their competance in the past.

#### ===

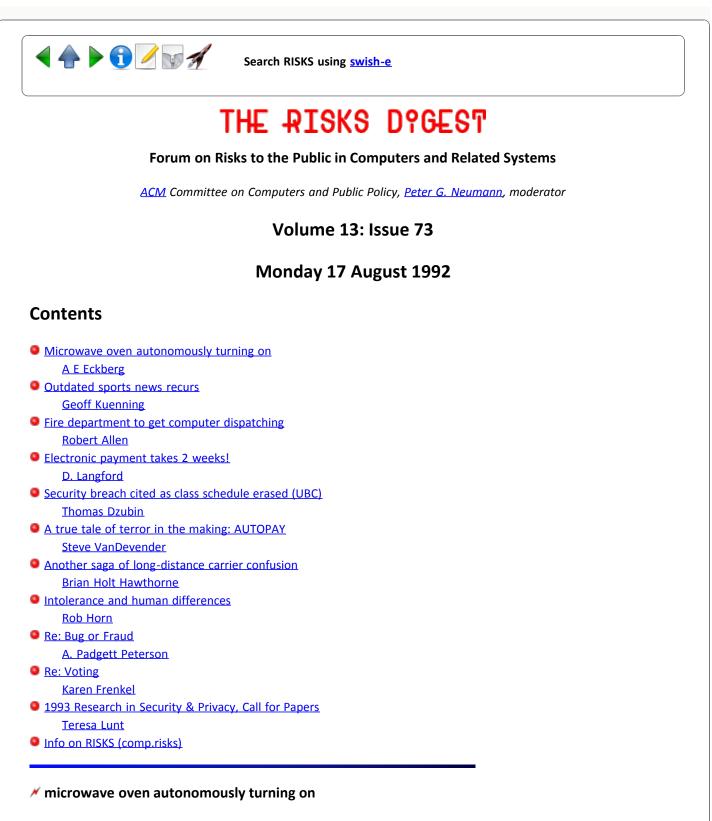
As for voice-mail systems, a simple "and dial 0 for an operator" entry in the menu would solve most of the problems people have. I \*like\* using these systems, but occasionally I get lost in a maze of twisty little options (say, for example, the menu item I'm used to selecting has been changed) and would dearly like the ability to bail out.

Peter da Silva, Taronga Park BBS, Houston, TX +1 713 568 0480/1032



Search RISKS using swish-e

Report problems with the web pages to the maintainer



A E Eckberg <ted@buckaroo.att.com> Mon, 17 Aug 92 05:57:44 EDT

This article was originally posted in 'misc.consumers' and 'misc.consumers.house', and a responder suggested also posting in 'comp.risks'.

I'm looking for information from anyone who has experienced an electronic-control appliance "autonomously" turning itself on or otherwise

doing something that it was not explicitly "commanded" to do by a user. Also, if anyone has not experienced this first-hand, but knows of such incidents, I'd like to know.

Here's why I'm looking for this information.

Recently, while we were out of the house, our electronic-control microwave oven turned itself on. While this oven has a timer, it had not been activated, and there was no "logical" reason for the microwave to turn on. There had been, however, an electrical storm in the area that was severe enough to have affected many of the computer systems where I work (about a mile from our home), and the only logical explanation for the microwave coming on was that its microprocessor control had received just the right impulses from the storm to set it running. We don't know how long the oven had been running when we came back, but when we entered the house the microwave was running and had burned/melted a plastic trim piece inside, and had filled the house with burned-plastic fumes.

In my opinion, electronic controls for appliances should be designed with more fail-safe capabilities than seem to be the case here, and it appears to me that our oven has a fundamental safety design flaw. Very likely ALL electronic-control appliances share this flaw, and there are likely to be severe consequences, although probably quite rare. In our case our house would probably have burned if we had not come back and turned the microwave off.

Because occurrences like this are probably very rare, and maybe even unbelievable, I'd like to hear from anyone else who could relate incidents similar to this that could add to the believability of what happened.

Please send relevant information to me at a.e.eckberg@att.com

#### ✓ Outdated sports news recurs

Geoff Kuenning <desint!geoff@uunet.UU.NET> Mon, 17 Aug 92 00:50:43 PDT

About a year ago, Hennessey's, a local bar, replaced the usual ESPN programming on one of their four TV monitors with an obviously computer-generated display giving the day's sports scores, standings, and miscellaneous news, as well as showing advertising and some simple graphics. I found it to be a nice addition, since ten minutes or so of watching would give me the results on my favorite teams.

This summer, the system has developed a rather troubling memory problem. There seems to be a flaw in the deletion of outdated information. In July, for example, it reported on the outcome of a Stanley Cup hockey game played in April, complete with a coach's comments on the (supposedly) next-scheduled game. This evening (August 16), it displayed baseball standings showing the Dodgers in fourth place, 6.5 games out of first. (As of this morning, they were in last place, 22 games behind. I guess today's loss to San Francisco really helped their standings!)

Even more interesting, the out-of-date results are mixed with up-to-date information. The incorrect baseball standings were followed by a Las Vegas odds display gaving information on the correct National League baseball schedule for Monday.

I have no idea how the system works (except that the immediacy of the results and the speed of the display update together indicate a local computer which receives information from a service via a modem), so I can't speculate on where the problem lies. But it's clear that somebody needs to erase the disk!

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

[Sounds as if there is a selective three month lag for certain results. OR, could it be that some of the data entry is done by people who write dates such as 7/4/92 to mean 7 April rather than July 4? PGN]

#### Fire department to get computer dispatching

rja@sun.com <Robert.Allen@eng.sun.com> Thu, 13 Aug 92 21:06:02 GMT

From a scanner hobbiest newsletter:

Hayward [California] Fire department is going to be going to all MDT dispatch in the future. According to Hayward Fire, they will never, ever, have to use voice traffic again. Even the Battalion Chief won't hear the calls since there will be no voice traffic calls. The Chief will have to be near a computer terminal to see the calls. This according to an anonymous source.

The risks should be obvious...

### ✓ Electronic payment takes 2 weeks!

"D.Langford" <dl1@ukc.ac.uk> Fri, 14 Aug 92 17:22:36 BST

I bank with one of the UK's largest building societies, the Nationwide. I was attracted by their advertising, which offered 'electronic payments' via their cashpoint machines. You notify details of the accounts you'll want to pay, and can then send money to pay the bills from any machine. It looked neat and fast, and I liked the idea of a paperless payment.

I'd used it to pay my credit card bills for about a year, when in May I needed to settle a Visa account of 600 pounds or so (\$1100). It was twelve days before the due date...

Yes, that's right. Although they debited my account immediately, they did not pay the credit card company for two weeks - and I incurred interest charges for not making a payment when I'd made it 2 weeks before.

This was NOT an accident, it wasn't a mistake - Nationwide told me that their terms and conditions permitted them to take up to TWO WEEKS to make an ELECTRONIC payment! The small print, which talks of 'working days' rather than 'real' days, bore this out. I'd - foolishly - always assumed payment would be made faster if I used an electronic cashpoint; this was several times slower than a paper transaction!

The RISKs are obvious; your money goes, but bills are not paid, and the bank doesn't tell you.

I asked for a technical explanation - writing a system which takes two weeks to process a payment sounded tricky to me. The eventual answer was so depressing it had to be true - mag tapes are moved physically around the UK, until they eventually arrive at the right location.

### Security breach cited as class schedule erased (UBC)

Thomas Dzubin <tdzubin@cue.bc.ca> Thu, 13 Aug 92 18:43:37 PDT

(From \_The Vancouver Sun\_ August 13, 1992. Article by Lynn Moore)

University of B.C. student Tamiko Musgrove thought the worst had happened when she checked on her class schedule for September and found she didn't have one. Only two weeks earlier, Musgrove had used UBC's telephone registration system and managed to get all nine courses she needed for her second year of study, including those hard-to-get labs. Someone, Musgrove concluded after a brief investigation, had breached the security of the Telereg system and wiped out her courses. A Telereg hotline operator told her someone using her student number and birth date entered the system one week after she chose her courses and dropped them one by one. And seven of the nine courses she wanted had filled up since then. Although Musgrove was quickly reinstated into her courses after assuring UBC it wasn't she who dropped them, she still wonders if Telereg security is up to snuff. UBC registration coordinator Sham Pendleton says it is and what happened to Musgrove is rare. "One or two students each year" claim their registration files have been tampered with through the Telereg System, Pendleton said. And Martin Ertl of the Alma Mater Society said Telereg security breaches have not been reported to the student association. Students should keep their eight-digit identification number to themselves, Pendleton said. That and their birth date combine to make the Telereg access code. "Chances of someone knowing that combination of numbers is very, very slim," she said. Student identification numbers have to be used on every assignment and lab that is handed in to be marked, countered Musgrove, and it would not difficult for a determined classmate to learn a student's number. Birth dates are a little more difficult to figure out but not impossible, said Musgrove, who believes that a male classmate who was harassing her last year erased her courses. Pendleton said that when cases like Musgrove's arise, students are put back into their original courses and given a new \_and fictitious\_ birthday. Students can also request that a new birth date be assigned to them if they fear their numbers are known to others, she said.

Thomas Dzubin, tdzubin@cue.bc.ca

# A true tale of terror in the making: AUTOPAY

Steve VanDevender <stevev@miser.uoregon.edu> Wed, 12 Aug 92 23:30:22 PDT

I work for a game software company in Eugene, Oregon. It has grown tremendously over the past year as a result of a successful series of products and a merger with another, larger company, going from 35 to 135 employees in about a year.

Traditionally, employees have been asked to hand in signed timesheet forms to report vacation and sick leave days taken and information on projects we were working on. During the last pay period the accounting department announced they were going to introduce a program called AUTOPAY that would run on the company-wide LAN to gather this information, and that eventually paper timesheets would be phased out.

Someone soon noticed that since you only needed to provide your LAN login name to AUTOPAY for identification, it was possible for anyone to view and modify anyone else's timesheet data. When I brought up my concerns to our chief financial officer while handing in my paper timesheet, I was assured that data from AUTOPAY would be checked before being entered into the payroll system. Later this person also responded to a public e-mail message noting that AUTOPAY had no security, saying that "the only reason someone would modify another person's timesheet would be to be mean or ornery." By now I had become concerned, and wrote an e-mail reply of my own saying that with that kind of attitude and no security, we were just waiting to be stung. I also noted that computer-gathered data of this type is all too often used without any verification. Even with verification it would still be possible to do subtle things like add vacation days a few at a time to someone else's timesheet until they were used up, resulting in at best confusion and at worst loss of pay when the person claimed real vacation time.

Since then we've gone through another pay period where password protection was hacked into the program. I promptly requested a password in person (the announcement asked people to send password requests in e-mail!), then discovered on returning to my office that I couldn't get it to work. I then tried something that I hoped wouldn't work, but suspected would -- I grepped the directory tree containing the AUTOPAY files for the first few characters of my password, and found it in one of the files. To my horror this file was publicly readable \_and writable\_; I could see other people's passwords and modify them if I had wanted to. All six characters (the maximum allowed!) were entered correctly in the password file but if I typed them into the program they would never match, although typing the first five would work. After I complained about the lack of access protection for the password file it was made read-only, which means that although now people can't change other's passwords, they can still find out what they are.

Unfortunately the head-in-the-sand approach to security exhibited by the accounting staff and some other participants in a small public e-mail discussion has been rewarded so far because no one has been malicious enough to

try screwing up the AUTOPAY data. I have gotten a bit frustrated that the attitude towards security for data that affects everyone's pay is so lax.

Another less drastic problem with this AUTOPAY system is that it has an unusually poor user interface, particularly when it comes to saving timesheet data and exiting the program--I usually have to run through it twice to make sure that my data has been entered properly because the method for exiting and the prompts given by the program are obscure. The individual author (whose name appears in a garish and pointless title screen) appears to know as little about user interface design as he does about security.

Although nothing has yet gone terribly wrong with AUTOPAY, it has all the ingredients of a minor computer security fiasco in the making. I hope that any sequels I write will be happier ones.

### Another saga of long-distance carrier confusion

Brian Holt Hawthorne <praxsys!moon!rowan@uunet.UU.NET> Mon, 10 Aug 92 09:53:41 EDT

Kraig Meyer reported on being switched from MCI to AT&T without any action on his part. We has something similar happen to us recently, but with an additional twist.

In February, MCI called our home and convinced my wife to sign us up for the MCI Friends & Family program, promising her \$20 of free long distance and that they would switch us back free to AT&T if we didn't like it. She asked them explicitly how the \$20 would be paid ("a credit on your first month's bill") and generally made sure they weren't trying to pull any tricks. I was surprised that several days later, we were on MCI, since I have a password on my New England Telephone account that they assured me would prevent anyone from making any changes without it. Risk number one: a supposedly secure system that allows unauthorized transactions if they come from certain sources that NET trusts, but I don't.

In early March, we received an envelope from MCI containing a \$5 certificate good only for our March bill, a \$5 certificate good only for April and a \$10 certificate good only on our May bill. I immediately called MCI and explained that this was unacceptable, and that I wasn't going to do business with a company that lied to us. I told them to switch us back to AT&T free like they had promised. I was told that I would have to call my local phone company for that change, that they could only switch people to MCI, not to other carriers. I asked them how they were going to pay for it, and they said "a credit on your bill". Risk number two: MCI claims to be unable to reverse their transactions.

I called NET and they agreed to switch me back to AT&T. Several days later, the 700 number that tells you your LD carrier told me I was on AT&T. When our March bill arrived, it had all LD calls billed by MCI. I called the 700 number, and sure enough, we were back on MCI.

NET looked up the change and told me that apparently MCI frequently puts through changes a couple of months in a row, to make sure that people really

get switched. They agreed to switch me back to AT&T immediately at no cost. They also told me not to pay for any of the calls billed by MCI after the date was supposed to have been switched to AT&T. Risk number three: Transactions are not verifiable, and are repeated.

A month later, our April bill arrived, and all of the LD charges were billed by...you guessed...MCI. We called NET who informed us MCI had pulled the same trick: apparently not many people take them up on their offer to switch back after a month. NET told us not to pay the LD charges (so we ended up getting the free LD service after all :-) and switched us BACK to AT&T. About this time I started getting entreating letters and phone calls from BOTH AT&T and MCI begging me to get back on their service. I was very short with MCI, and had to try very hard to convince that AT&T telemarketers that I really was on AT&T and they weren't going to pick up a commission on me. Risk number four: telemarketing databases that seem out-of-date with customer records.

When our May bill arrived, our LD calls were billed by MCI. This time NET assured us that we really were on AT&T and they would look into it. They told us to pay the bill (over my protestations). The 700 number told us we were on AT&T.

Our June bill was also billed by MCI, and this time we managed to talk to someone at NET who took an intellectual interest in what was happening, and tracked things down. Apparently, NET had us correctly connected to AT&T's LD network, and everytime we called, the technicians would check the configuration on our number and see that we had already been changed to AT&T and do nothing. The billing system, however, had failed to notify AT&T that we were back on their network, and had also failed to notify MCI that we were off of their network. Moreover, NET's billing system actually thought we were on MCI.

Our July bill correctly showed us on AT&T for the latter part of the month.

Question: does this mean that NET generates the billing data for LD calls dialed, rather than the company that is actually carrying those calls??

rowan@praxsys.com +1.617.255.9600x132

### Intolerance and human differences

<HORN%athena@leia.polaroid.com> Wed, 12 Aug 1992 15:39 EST

System designers will need much more understanding of diversity (not the PC kind) as computer based systems go into widespread use. The somewhat intolerant comments regarding user inability to understand obvious systems are indications of design flaws. There are some people who are stupid, and others who have learned to use feigned stupidity as a negotiating mechanism, but most of these problems are related to different personality traits.

As a basic, I recommend that anyone working with such systems really learn about how different people can be. The Hermann Brain dominance profile (left-right brain) and the Myers-Briggs profiles are two important ways to discuss some aspects of differences. There are also many other more discipline specific analyses of such things as human behavior under stress, etc. Reading the literature is a start, but the organized training courses are very important. Take one if possible. You may learn a lot about how differently react and how differently they want to be treated.

One of the classic examples is between the analytic left-brained engineer who insisted on a detailed theoretical training method. His customers were physically oriented lower-left brain sensor types. They wanted someone to take them to the machine, literally hold their hands, have them push the buttons, and directly experience the machine. The engineer felt that this would be a very demeaning experience, while they thought the lecturing was worthless and insulting. A simple personality difference.

Also, don't forget the impact of age, illness, stress, and the like on behavior. Now that more of us have grey hairs you see more computers that are usable by bifocal wearers. Rob Horn

[For more on the left-brain / right-brain differentiation, see my chapter, Psychosocial Implications of Computer Software Development and Use: Zen and the Art of Computing, in Theory and Practice of Software Technology, edited by Ferrari, Bolognani, and Goguen, North-Holland, pp. 221-232, 1983. PGN]

## Re: Bug or Fraud (<u>RISKS-13.72</u>)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Wed, 12 Aug 92 15:29:49 -0400

- > [Once again this brings up the concern of people thinking that anything that
- > happens in a computer system that wasn't expected by the end users is a bug.
- > I'd like a job where I got paid \$7000 to remove a "conditional statement."

Back before the flood there used to be a joke about the computer repairman (person?) that , when called to fix a problem, disappeared inside the computer with a little silver hammer. Shortly there can a musical \*tonk\* from inside and all of the lights began to blink.

Emerging, the repairman presented the owner with a bill for US\$ 25000.25. The owner protested and requested an itemized bill. The repairman complied with the following: Striking computer: US\$ .25 Knowing where to strike computer: US\$ 25000.00

I have yet to have anyone complain about my prices to cure a virus. Padgett

# Ke: Voting (Mercuri, <u>RISKS-13.72</u>)

<KARENF@acmvm.bitnet> Wed, 12 Aug 92 16:27:42 EDT

Rebecca Mercuri has given the wrong address for the hearing on voting machines

that is to take place on Aug. 20. The correct address is: 42 Broadway, which is downtown near Battery Park City. This hearing is for the press and is a contract briefing. The second hearing, on Sept. 10, is open to the public.

## 1993 Research in Security & Privacy, Call for Papers

Teresa Lunt <lunt@csl.sri.com> Fri, 14 Aug 92 11:39:27 -0700

CALL FOR PAPERS

1993 IEEE Symposium onMay 24-26, 1993Research in Security and PrivacyOakland, California

sponsored by IEEE Computer Society Technical Committee on Security and Privacy in cooperation with The International Association for Cryptologic Research (IACR)

The purpose of this symposium is to bring together researchers and developers who work on secure computer systems. The symposium will address advances in the theory, design, implementation, evaluation, and application of secure computer systems. Papers and panel session proposals are solicited in the following areas:

Secure Systems	Privacy Issues	Information Flow
Network Security	Formal Models	Viruses and Worms
Database Security	Access Controls	Security Verification
Authentication	Data Integrity	Auditing and

#### **INSTRUCTIONS TO AUTHORS:**

Send six copies of your paper and/or panel session proposal to Richard Kemmerer, Program Co-Chair, at the address given below. Put names and affiliations of authors on a separate cover page only, as a ``blind'' refereeing process is used. Abstracts, electronic submissions, late submissions, and papers that cannot be published in the proceedings will not be accepted.

Papers must be received by November 15, 1992 and must not exceed 7500 words; papers that exceed this length will be rejected without review. Authors will be required to certify prior to December 25, 1992 that any and all necessary clearances for publication have been obtained. Authors will be notified of acceptance by February 1, 1993. Camera-ready copies are due not later than March 15, 1993.

The Symposium will also include informal poster sessions. Send one copy of your poster session paper to Teresa Lunt, at the address given below, by January 31, 1993. Electronic submission of the latex source for poster session papers is strongly encouraged. Poster session authors must send a

certification with their submittal that any and all necessary clearances for publication have been obtained.

#### PROGRAM COMMITTEE

Tom Berson Paul Karger Jon Millen MITRE Anagram Laboratories OSF Tanya Korelsky Deborah Cooper Jeff Picciotto Paramax Systems Corporation ORA MITRE George Dinolt Sue Landauer Phillip Porras Loral Labs TIS Aerospace Virgil Gligor Ravi Sandhu Teresa Lunt University of Maryland SRI George Mason Univ. Deborah Hamilton Doug McIlroy Marv Schaefer Hewlett-Packard Laboratories AT\&T Bell Labs CTA Jeremy Jacob John McLean **Brian Snow** Oxford University NRL NSA Sushil Jajodia Catherine Meadows Yacov Yacobi George Mason University NRL Bellcore

For further information concerning the symposium, contact:

Teresa Lunt, General Chair	Cristi E. Garvey, Vice Chair
SRI International, EL245	TRW, MS R2-2104
333 Ravenswood Avenue	One Space Park
Menlo Park, CA 94025	Redondo Beach, CA 90278
Tel: (415)859-6106	Tel: (310)812-0566
FAX: (415)859-2844	FAX: (310)812-7147
lunt@csl.sri.com	

Richard Kemmerer, Program Co-ChairJohn Rushby, Program Co-ChairComputer Science DepartmentSRI International, EL254University of California333 Ravenswood AvenueSanta Barbara, CA 93106Menlo Park, CA 94025Tel: (805)893-4232Tel: (415)859-5456FAX: (805)893-8553FAX: (415)859-2844kemm@cs.ucsb.edurushby@csl.sri.com

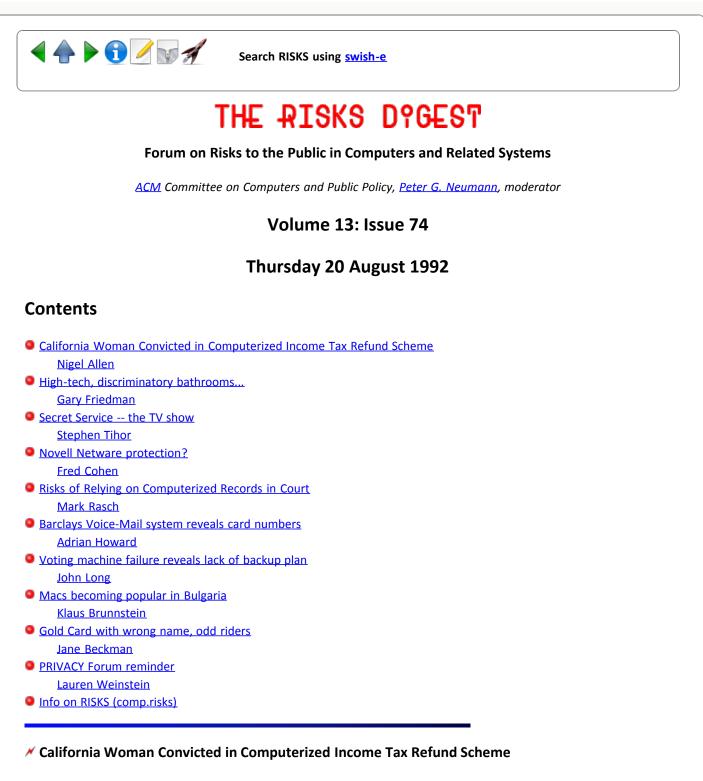
Jeremy Jacob, European Contact Oxford Univ. Computing Laboratory 11 Keble Road Oxford, England OX1 3QD Tel: +44 865 272562 FAX: +44 865 273839 jeremy.jacob@prg.oxford.ac.uk

🖣 🛖 🕨 🕤 🥖 🐨 🚀

Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 13: Issue 73



<Nigel.Allen@lambada.oit.unc.edu> Tue, 18 Aug 92 23:34:25 EDT

Here is a press release from the U.S. Justice Department.

California Woman Convicted in Income Tax Refund Scheme To: National Desk, California Correspondent Contact: U.S. Department of Justice, 202-514-2007

FRESNO, Calif., Aug. 18 /U.S. Newswire/ -- Acting Assistant Attorney General

James A. Bruton and the United States Attorney for the Eastern District of California, George L. O'Connell, announced Monday, Aug. 17, that Enedina Ochoa of Turlock, Calif., 26, was convicted by a federal jury on Friday, Aug. 14, of one count of conspiracy to defraud the government and 20 counts of assisting others in filing false income tax refund claims with the Internal Revenue Service.

The jury trial lasted four days before United States District Judge Oliver W. Wanger. Wanger ordered Ochoa held in custody pending sentencing. Ochoa's scheme exploited the Internal Revenue Service's newly implemented electronic filing system, which allows filers of refund claims to receive their refund checks in one or two days. By causing large numbers of false refund claims to be electronically filed, Ochoa and her co-conspirator, Karleena Pulido, fraudulently obtained approximately \$100,000 from the Internal Revenue Service. Most of the criminal activity involved 1991 federal income tax returns filed earlier this year.

Ochoa and Pulido, a Turlock income tax preparer who pled guilty two weeks ago to conspiracy to defraud the government and 29 counts of assisting others in filing false claims for income tax refunds, engaged in a scheme to electronically file false refund claims with the I.R.S. by recruiting individuals to provide their real names and social security numbers for use by Pulido on false Forms W-2 which Pulido fabricated. Ochoa then assisted the recruited individuals in electronically filing these false refund claims with the I.R.S. from electronic return transmitters such as Cash-N-Dash, an income tax transmittal and check cashing service headquartered in Fresno. Ochoa and Pulido then divided divided the refund proceeds among themselves and the individuals they recruited.

The long-standing I.R.S. system of filing paper returns requires a taxpayer to wait several weeks before receiving a refund check.

Ochoa and Pulido face a maximum sentence of ten years imprisonment and a fine of \$250,000 for the conspiracy convictions and five years imprisonment for each conviction of assisting in the filing of a false claim. Sentencing is set for Oct. 19, and Oct. 26, for Pulido and Ochoa, respectively, before Wanger.

The case is the result of an extensive and ongoing investigation of electronic filing fraud by special agents of the Internal Revenue Service's Criminal Investigation Division, and was prosecuted by Department of Justice Tax Division Trial Attorneys Eric C. Lisann and Floyd J. Miller. It is the first prosecution of this type of crime in this judicial district, and is one of only a very few such cases that have gone to trial anywhere in the United States since the inception of the Internal Revenue Service's electronic filing system.

Acting Assistant Attorney General James Bruton stated, "This conviction serves as notice that the federal government is committed to early detection and prosecution of electronic filing schemes. Blatant abuse of the Internal Revenue Service's computerized refund program will not be tolerated." According to Rick Speier, chief of the Internal Revenue Service's Criminal Investigation Division in San Jose and Fresno, "as the use of electronic filing increases, the Internal Revenue Service will continue to be vigilant in identifying electronic filing schemes organized by unscrupulous individuals who seek to exploit the system for criminal purposes."

High-tech, discriminatory bathrooms...

Gary Friedman <garyf@puente.Jpl.Nasa.Gov> Mon, 17 Aug 92 15:24:12 PDT

The Santa Monica, CA Municipal Pier has recently added new "high-tech" public restrooms that are discriminatory about to whom they will dispense water. Like many of the new breed of restrooms increasingly found in airports, both the urinals and the washbasins have an infrared proximity sensor which turns the water on and off for you; there's no need to ever touch a control.

A nine-year-old who was with me stood in front of a washbasin I had just used, and got mad when the faucet wouldn't turn on for him. Nothing he tried, including covering the sensor with his hand, would work. Only after I suggested jumping up and down and waving his hands above his head did the faucet finally acknowledge that a human was there and grant the public resource, and then promptly quit a few seconds later when his hands moved down to be washed.

I know the problem of people leaving conventional faucets running unattended is ancient, and that many solutions have been tried in the past to combat it; such as the mechanical push button which will let the water run for anywhere from 1 to 15 seconds, depending on the maintenance history. I see in this new electronic twist to an old problem two new RISKS, one of which is rather serious:

1) Discrimination against short people. This being a public area, it is reasonable to expect children. (It's doubtful that any health epidemic might result from this; after all most kids don't wash their hands and don't prepare food in eating establishments.)

2) I saw no manual overrides for the controls; I assume that if a power failure were to occur (as a result of a natural disaster; not difficult to imagine in California) it would also cut off the water delivery, a crucial resource during such times. Often during a disaster the electricity is the first thing to go out, while the water flow is much more reliable. This new solution unnecessarily couples the two while providing no perceivable advantages over the older mechanical methods, exacerbating worst-case scenarios.

(This gets added to my ever-expanding list encompassing electronic tire pressure gages, electronic carpenter's level, computerized office building directories, microprocessor-based wire strippers, etc. for having no advantages over the prior art but catastrophically fail when the batteries die.)

#### -Gary Friedman

Gary Friedman, Jet Propulsion Laboratory - NASA, 4800 Oak Grove Drive, Pasadena, CA 91109 (818) 306-6193 {cit-vax,elroy,psivax}!devvax!garyf

# ✓ Secret Service -- the TV show

Stephen Tihor 212 998 3052 <TIHOR@ACFcluster.NYU.EDU> 17 Aug 1992 12:24:24 -0400 (EDT)

Last night NBC broadcast an episode of "Secret Service" in NY at least that

featured a straightforwards nut who wants to kill the President plot and then a rather confusing account of their high technology defense of a fuzzy city power system against sabotage by a fired employee.

I hope someone taped it and caught the exact wording of the disclaimer at the end because it was hard to follow the logic and determine what was the original incident and what was Hollywoodisms.

The piece was prefaced with a brief discussion some of the risks of power outages.

The expert quickly diagnosed the problem as a VIRUS. Persistent references to virus in the context of a electric power control system seemed odd. Since they appeared to be running pre-existing VIRUS checking software on the system one might suspect the "main frame" was an IBM PC or Apple Macintosh running standard software rather than a real tiem control system or perhaps something larger and safer. Interesting references were made to viruses lurking WITHIN modems. Then they identified the source of the attacking codes as the local font storage in what appeared to be a old DECwriter dot matric printer.

With some external clues the agents attempt to confront the criminal in house, which is wired with many falling metal screen, sounds effects, and gas but which lacks reinfored walls. The culprit is classic middle aged computer geek who appears uncaring about possible loss of life although the agents do not mention to him the risk of a life sentence of death penalty of others die as a result of his sabotage. He refuses to help them disarm the problem.

The expert has announced that this is a logic bomb and eventually realizes that since the bug code is not in the copy of the system on disk as long as they shutdown without writing memory to disk they can reboot bug free. So a brief deliberate blackout is used to save the city.

I am obvious very curious about the TRUE FACTs of this can if the show plans to show such other SS triumphs in the war on electronic crime as almost destroying Steve Jackson Games.

[Program also noted by johana!tsw@apple.com (Tom Watson)]

# Movell Netware protection?

Mr Fred Cohen <cohen@fitmail.fit.qut.edu.au> Wed, 19 Aug 92 8:28:12 EST

I have been doing exhaustive tests on Novell Netware protection, and I cannot believe these people can sell their product on the basis that it is the most secure. If it is, we are in big trouble!!

 "Read Only" files are successfully infected by DOS viruses!
 "Directory protection" works exactly the opposite of how the manual claims! IN 3 DIFFERENT PLACES!!!
 Several protection bits work from a MacIntosh, but not from DOS machines!! What kind of network protection doesn't work when the user uses a different machine to login?!? Protection based in the user's machine and not on the server!!!

A shareware product successfully gathers passwords from the net as they are entered by the users! For \$35 I can get every password on your network (if I choose to pay the shareware licensing fees to be honest about it)
Passwords can be ANYTHING - including nothing at all! The supervisor password on our network is empty, so anyone on the net can login with no password (we are physically isolated - but how about some password controls!)
So-called Execute Only protection does not prevent companion viruses from working, and prevents the sys admin from verifying program integrity, prevents backup and restore of execute-only files, and thus is a great hindrance to protection!

This was the results of the first 2 DAYS of experiments! If we can find this many problems in 2 days (while not explicitly trying to look for these kinds of holes), I can't imagine anyone claiming this system to be the best available security. But who knows? In the next few days we will be looking at Unix based servers! FC

### **X** Risks of Relying on Computerized Records in Court

<Rasch@DOCKMASTER.NCSC.MIL> Wed, 19 Aug 92 11:46 EDT

Joe Konstan reports that CALL TRACE would pick up the identity of the individual responsible for making the harassing telephone calls even if RETURN CALL did not. He notes that "the switch does know who placed the call..." However, this assumes that the switch itself (which is computer software, after all) is operating properly, and isn't the cause of the problem. Even assuming no "bug" in the switch, there is always the (very real) danger that the switch can be compromised by unauthorized users (insiders or "hackers"). What this teaches us is that, as computerized systems become more vulnerable to attack and compromise, their reliability is compromised.

As a lawyer and former (computer crime) prosecutor, I can assure you that computerized information is \*routinely\* accepted as reliable and frequently forms the basis for criminal prosecutions and convictions. Telephone toll records, credit card records, bank statements and the like are admitted into evidence as "business records" without even a fleeting inquiry into the manner in which they were created. For the most part, Courts "assume" that these records are reliable. While computerized summaries and computer generated reports (created for litigation) are subject to greater scrutiny, they all suffer from the MEGO effect (My Eyes Glaze Over). If I can't understand it, it must be right.

Generally, there is little harm to this. For the most part, computer generated records are reliable, and are relied upon in the ordinary course of business transactions. Indeed, they are frequently more reliable than the "paper" records they replaced and which were routinely accepted. However, the public must be ever vigilant against the possibility of alterations, misinterpretations, and simple errors in these records -- they are not always

what they seem.

Mark D. Rasch, Arent Fox Kinter Plotkin & Kahn, Washington, D.C. (202) 857-6154 Rasch@ncsc.dockmaster.mil

#### **\*** Barclays Voice-Mail system reveals card numbers

Adrian Howard <adrianh@cogs.sussex.ac.uk> Wed, 19 Aug 92 09:48:34 +0100

>From the 18/08/1992 issue of the "Independent" (a "quality" English newspaper.) All transcription mistooks are, of course, my own.

Hackers pinpoint card weaknesses (John Eisenhammer --- Bonn)

Barclays Bank executives in Germany were forced to admit yesterday that young hackers had made a fool of their credit card computer system.

According to Hans-Hermann Schra"der, the official responsible for the Protection of Information regulations in the state of Hamburg, where the "crime" took place, the bank's computer security was "totally unsatisfactory".

For the past few months, a group of youths in Hamburg have been drawing out information about individual Visa and Eurocard owners, including their credit ratings, in order to show how easily such allegedly confidential information can be used.

Even worse for the bank, which has been running a massive advertising campaign in Germany for its offer of both main credit cards for the price of one, officials still cannot tell from the voice-mail computer records that anything was amiss. It was only after hearing tapes on television, with client voices on them, that Barclays officials conceded that all was not as it should be.

The special voice-mail computer was used by clients confirming that they had received their cards, at which point they provided their personal numbers, and by those requesting a credit limit increase. The information was recorded, not on normal tape but digitally by a computer, and the information was later decoded by bank staff. According to Rolf Wo"rdemann, a member of Germany's main hacker organisation, the Hamburg Chaos Computer Club, voice-mail computers such as the one at Barclays are as "easy to break as a bicycle lock".

Rather than prosecute Barclays officials are hoping that the hackers will be willing to co-operate, so that the bank can find out just how bad things are, and who needs new credit cards, The fact that the enterprising youths also managed, once they had accessed Barclays' computer system, to make lengthy international telephone calls at the bank's expense, will be quietly forgotten.

I found this especially amusing since Barclays officials have recently been appeared on national news in the UK expounding the infallibility of cash-card machines. I find the automatic assumption the computer cannot be fouling up exceptionally irritating. The thought of having to give personal numbers over the phone is also a bit of a worry (to me anyway --- but then I'm paranoid :-)

I also dislike the idea that the bank is having to ask the hackers how they did it. Shouldn't they have the expertise to find holes as apparently large as exist in the system (then again if they had the expertise, the holes wouldn't be there.) The "hackers" in the article, while not exactly represented as heros, are definitely not painted as villains either. I'm not so sure.

Oh well, another Infallible-Banking-Computer-System (tm) bites the dust! aids (email: adrianh@cogs.susx.ac.uk)

## Voting machine failure reveals lack of backup plan

# John (J.O.F.) Long <JLONG@BNR.CA> 17 Aug 92 14:46:00 EDT

This year, I started serving as a registrar for my precinct. Our county started using computerized tallying machines this year, and everyone had to go through required training to learn how to use them. During the training meeting, I asked what would happen if a machine should completely fail. I was assured that this "probably" would never happen. I could swear that some of the sample tallying machines in the back were snickering after this remark.

If there is a blackout to the machines, then voters are supposed to put their ballots into a special slot just for such emergencies. It is assumed that the electricity will come on again later during the day. (What if the power goes out 10 minutes before closing?) After the polls close, the registrar and judges are then supposed to open the special slot and send the ballots through the reader. Ballots cannot be read twice because the machine marks them as they go through.

The machines worked fine during the primary, but during the runoff, in which very few people voted, my machine had a memory error just a few minutes before closing. There was nothing that could be done except send another machine out to me. We only had 21 people vote the entire day (!), so we could have counted it by hand, but the elections board wouldn't allow it!

What if there had been several memory failures during the day? Would there be enough backup machines to handle it? What a mess! And why are we so reliant on machines that we cannot allow humans to do something that we can do just as quickly?

John Long, Raleigh, NC, jlong@bnr.ca

# Macs becoming popular in Bulgaria

<brunnstein@rz.informatik.uni-hamburg.dbp.de> 18 Aug 92 18:59 +0100

According to a report from Vesselin Bontchev who just returned from his summer vacation in Bulgaria, Macintoshs are becoming quite popular in Bulgaria. Recently, an Apple distributor began to distribute Macs which many Bulgarians found superior to their PC clones and began to like. We strongly hope that this may not attract the interest of the well-known virus authors in Bulgaria and subsequently in other Eastern European countries.

Klaus Brunnstein, University of Hamburg, Germany (August 18, 1992)

### ✓ Gold Card with wrong name, odd riders

Jane Beckman <jane@stratus.swdc.stratus.com> Mon, 17 Aug 92 15:46:49 PDT

Everyone gets credit card "pre-approval" offers in the mail, but this last one started me wondering. First off, it was addressed to "Jeffery L. Beckmann," with my correct address, down to a zip +4 code. My name is Beckman, not Beckmann (two n's), and my name is Jane G., not Jeffery L. And we won't even go into the way that my gender has gotten switched. So, how did Mr. Beckmann get associated with MY address in whomever's database?

Just for grins, to see what sort of gold Mastercard he was being offered, I read the thing. It had a \$10,000 credit line, and NO ONE, repeat, no one, has \*ever\* offered Beckman, Jane G. a card with that kind of credit line. Weirder still, to get the card, you were \*required\* to take out a cash advance of a minimum of \$2000, up to the \$10,000 limit of the card. After much searching through fine print, I found the card was offered by an institution called "First Deposit." Then I found the weirdest part---the terms would only be sent to you when you sent for your pre-approved cash advance and activated the Gold Card. In short, it could be 50% annual interest, starting to accrue from the time they send you your "advance," and you wouldn't even know it until you had taken the plunge. Even the form was strange---just a signature line and a phone number are to be provided. Normally, these forms ask for independent confirmation of credit---the usual questions about your obligations, etc., even if they are theoretically "pre-approved" (which is actually a misnomer).

Several things occur to me. I could sign Jeffery Beckmann up, collect his cash advance, and skip town, if I were that sort. Who would be responsible? The mysterious Mr. Beckmann, who may not exist? For that matter, what if Jeffery Beckmann's obligations and credit history get mixed up with mine, since his address is obviously already mixed up? And speaking of, HOW did this mystery person get HIS name associated with MY address, aside from a totally superficial resemblence between last names, his not even being spelled the same as mine? What if Mr. Beckmann is an international representative of a drug cartel, and now has his address linked to mine? Will my house suddenly be of interest to some unknown authorities, who are doing computer traces of his activities? What database generated this so generous invitation, and how did it determine that Mr. Beckmann was able to qualify for such a hefty cash advance/credit limit without even knowing his real address? The RISKS here seem to cover several different aspects of our overly- databased society.

-Jane G. Beckman [jane@swdc.stratus.com]

# PRIVACY Forum reminder

Lauren Weinstein <lauren@cv.vortex.com> Tue, 18 Aug 92 11:06 PDT

[Lauren Weinstein is urging people to submit their PRIVACY related stories, questions, comments, etc. to his PRIVACY Forum. Apparently not many people know of its existence, or else to consider privacy only in the more general context of RISKS. PGN]

You can get info about the digest by sending a message to:

privacy-request@cv.vortex.com

with the words:

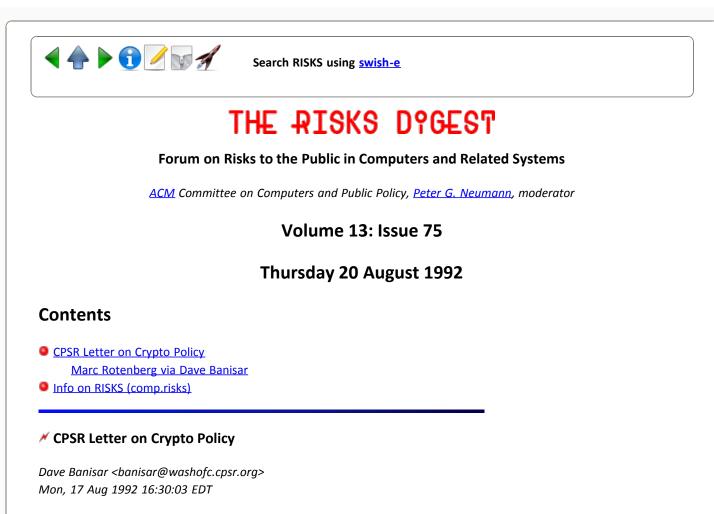
information privacy

in the BODY of the message. Submissions are explicitly solicited! --Lauren--



Search RISKS using swish-e

Report problems with the web pages to the maintainer



The following is the text of a letter Computer Professionals for Social Responsibility (CPSR) recently sent to Rep. Jack Brooks, chairman of the House Judiciary Committee. The letter raises several issues concerning computer security and cryptography policy. For additional information on CPSR's activities in this area, contact banisar@washofc.cpsr.org. For information concerning CPSR generally (including membership information), contact cpsr@csli.stanford.edu.

------

August 11, 1992

Representative Jack Brooks Chairman House Judiciary Committee 2138 Rayburn House Office Bldg. Washington, DC 20515-6216

Dear Mr. Chairman:

Earlier this year, you held hearings before the Subcommittee on Economic and Commercial Law on the threat of foreign economic espionage to U.S. corporations. Among the issues raised during the hearings were the future of computer security authority and the efforts of government agencies to restrict the use of new technologies, such as cryptography. As a national organization of computer professionals interested in the policies surrounding civil liberties and privacy, including computer security and cryptography, CPSR supports your efforts to encourage public dialogue of these matters. Particularly as the United States becomes more dependent on advanced network technologies, such as cellular communications, the long-term impact of proposed restrictions on privacy-enhancing techniques should be carefully explored in a public forum.

When we had the opportunity to testify before the Subcommittee on Legislation and National Security in May 1989 on the enforcement of the Computer Security Act of 1987, we raised a number of these issues. We write to you now to provide new information about the role of the National Security Agency in the development of the Digital Signature Standard and the recent National Security Directive on computer security authority. The information that we have gathered suggests that further hearings are necessary to assess the activities of the National Security Agency since passage of the Computer Security Act of 1987.

The National Security Agency and the Digital Signature Standard

Through the Freedom of Information Act, CPSR has recently learned that the NSA was the driving force behind the selection and development of the Digital Signature Standard (DSS). We believe that the NSA's actions contravene the Computer Security Act of 1987. We have also determined that the National Institute of Standards and Technology (NIST) attempted to shield the NSA's role in the development of the DSS from public scrutiny.

The Digital Signature Standard will be used for the authentication of computer messages that travel across the public computer network. Its development was closely watched in the computer science community. Questions about the factors leading to the selection of the standard were raised by a Federal Register notice, 56 Fed. Reg. 42, (Aug 30, 1991), in which NIST indicated that it had considered the impact of the proposed standard on "national security and law enforcement," though there was no apparent reason why these factors might be considered in the development of a technical standard for communications security.

In August 1991, CPSR filed a FOIA request with the National Institute of Standards and Technology seeking all documentation relating to the development of the DSS. NIST denied our request in its entirety. The agency did not indicate that they had responsive documents from the National Security Agency in their files, as they were required to do under their own regulations. 15 C.F.R. Sec. 4.6(a)(4) (1992). In October 1991, we filed a similar request for documents concerning the development of the DSS with the Department of Defense. The Department replied that they were forwarding the request to the NSA, from whom we never received even an acknowledgement of our request.

In April 1992, CPSR filed suit against NIST to force disclosure of the documents. CPSR v. NIST, et al., Civil Action No. 92-0972-RCL (D.D.C.). As a result of that lawsuit, NIST released 140 out of a total of 142 pages. Among those documents is a memo from Roy Saltman to Lynn McNulty which suggests that there were better algorithms available than the one NIST eventually recommended for adoption. If that is so, why did NIST recommend a standard that its own

#### expert believed was inferior?

Further, NIST was required under Section 2 of the Computer Security Act to develop standards and guidelines to "assure the cost-effective security and privacy of sensitive information in federal systems." However, the algorithm selected by NIST as the DSS was purposely designed to minimize privacy protection: its use is limited to message authentication. Other algorithms that were considered by NIST included both the ability to authenticate messages and the capability to incorporate privacy-enhancing features. Was NSA's interest in communication surveillance one of the factors that lead to the NIST decision to select an algorithm that was useful for authentication, but not for communications privacy?

Most significantly, NIST also disclosed that 1,138 pages on the DSS that were created by the NSA were in their files and were being sent back to the NSA for processing. Note that only 142 pages of material were identified as originating with NIST. In addition, it appears that the patent for the DSS is filed in the name of an NSA contractor.

The events surrounding the development of the Digital Signature Standard warrant further Congressional investigation. When Congress passed the Computer Security Act, it sought to return authority for technical standard-setting to the civilian sector. It explicitly rejected the proposition that NSA should have authority for developing technical guidelines:

Since work on technical standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards job from the [National Institute of Standards and Technology]. By putting the NSA in charge of developing technical security guidelines (software, hardware, communications), [NIST] would be left with the responsibility for only administrative and physical security measures -- which have generally been done years ago. [NIST], in effect, would on the surface be given the responsibility for the computer standards program with little to say about the most important part of the program -- the technical guidelines developed by NSA.

Government Operation Committee Report at 25-26, reprinted in 1988 U.S. Code Cong. and Admin. News at 3177-78. See also Science Committee Report at 27, reprinted in 1988 U.S.C.A.N. 3142.

Despite the clear mandate of the Computer Security Act, NSA does, indeed, appear to have assumed the lead role in the development of the DSS. In a letter to MacWeek magazine last fall, NSA's Chief of Information Policy acknowledged that the Agency "evaluated and provided candidate algorithms including the one ultimately selected by NIST." Letter from Michael S. Conn to Mitch Ratcliffe, Oct. 31, 1991. By its own admission, NSA not only urged the adoption of the DSS -- it actually "provided" the standard to NIST.

The development of the DSS is the first real test of the effectiveness of

the Computer Security Act. If, as appears to be the case, NSA was able to develop the standard without regard to recommendations of NIST, then the intent of the Act has clearly been undermined.

Congress' intent that the standard-setting process be open to public scrutiny has also been frustrated. Given the role of NSA in developing the DSS, and NIST's refusal to open the process to meaningful public scrutiny, the public's ability to monitor the effectiveness of the Computer Security Act has been called into question.

On a related point, we should note that the National Security Agency also exercised its influence in the development of an important standard for the digital cellular standards committee. NSA's influence was clear in two areas. First, the NSA ensured that the privacy features of the proposed standard would be kept secret. This effectively prevents public review of the standard and is contrary to principles of scientific research.

The NSA was also responsible for promoting the development of a standard that is less robust than other standards that might have been selected. This is particularly problematic as our country becomes increasingly dependent on cellular telephone services for routine business and personal communication.

Considering the recent experience with the DSS and the digital cellular standard, we can anticipate that future NSA involvement in the technical standards field will produce two results: (1) diminished privacy protection for users of new communications technologies, and (2) restrictions on public access to information about the selection of technical standards. The first result will have severe consequences for the security of our advanced communications infrastructure. The second result will restrict our ability to recognize this problem.

However, these problems were anticipated when Congress first considered the possible impact of President Reagan's National Security Decision Directive on computer security authority, and chose to develop legislation to promote privacy and security and to reverse efforts to limit public accountability.

#### National Security Directive 42

Congressional enactment of the Computer Security Act was a response to President Reagan's issuance of National Security Decision Directive ("NSDD") 145 in September 1984. It was intended to reverse an executive policy that enlarged classification authority and permitted the intelligence community broad say over the development of technical security standards for unclassified government and non-government computer systems and networks. As noted in the committee report, the original NSDD 145 gave the intelligence community new authority to set technical standards in the private sector:

[u]nder this directive, the Department of Defense (DOD) was given broad new powers to issue policies and standards for the safeguarding of not only classified information, but also other information in the civilian agencies and private sector which DOD believed should be protected. The National Security Agency (NSA), whose primary mission is one of monitoring foreign communications, was given the responsibility of managing this program on a day-to-day basis.

H. Rep. No. 153 (Part 2), 100th Cong., 1st Sess. 6 (1987). The legislation was specifically intended to override the Presidential directive and to "greatly restrict these types of activities by the military intelligence agencies ... while at the same time providing a statutory mandate for a strong security program headed up by [NIST], a civilian agency." Id. at 7.

President Bush issued National Security Directive ("NSD") 42 on July 5, 1990. On July 10, 1990, Assistant Secretary of Defense Duane P. Andrews testified before the House Subcommittee on Transportation, Aviation, and Materials on the contents of the revised NSD. The Assistant Secretary stated that the "the new policy is fully compliant with the Computer Security Act of 1987 (and the Warner Amendment) and clearly delineates the responsibilities within the Federal Government for national security systems."

On August 27, 1990, CPSR wrote to the Directorate for Freedom of Information of the Department of Defense and requested a copy of the revised NSD, which had been described by an administration official at the July hearing but had not actually been disclosed to the public. CPSR subsequently sent a request to the National Security Council seeking the same document. When both agencies failed to reply in a timely fashion, CPSR filed suit seeking disclosure of the Directive. CPSR v. NSC, et al., Civil Action No. 91-0013-TPJ (D.D.C.).

The Directive, which purports to rescind NSDD 145, was recently disclosed as a result of this litigation CPSR initiated against the National Security Council.

The text of the Directive raises several questions concerning the Administration's compliance with the Computer Security Act:

1. The new NSD 42 grants NSA broad authority over "national security systems." This phrase is not defined in the Computer Security Act and raises questions given the expansive interpretation of "national security" historically employed by the military and intelligence agencies and the broad scope that such a term might have when applied to computer systems within the federal government.

If national security now includes international economic activity, as several witnesses at your hearings suggested, does NSD 42 now grant NSA computer security authority in the economic realm? Such a result would clearly contravene congressional intent and eviscerate the distinction between civilian and "national security" computer systems.

More critically, the term "national security systems" is used throughout the document to provide the Director of the National Security Agency with broad new authority to set technical standards. Section 7 of NSD 42 states that the Director of the NSA, as "National Manager for National Security Telecommunications and Information Systems Security," shall \* \* \*

c. Conduct, \*approve\*, or endorse research and development of techniques and equipment to secure national security systems.

d. Review and \*approve\* all standards, techniques, systems, and equipment, related to the security of national security systems.

\* \* \*

h. Operate a central technical center to evaluate and
 \*certify\* the security of national security
 telecommunications and information systems.

#### (Emphasis added)

Given the recent concern about the role of the National Security Agency in the development of the Digital Signature Standard, it is our belief that any standard-setting authority created by NSD 42 should require the most careful public review.

2. NSD 42 appears to grant the NSA new authority for information security. This is a new area for the agency; NSA's role has historically been limited to communications security. Section 4 of the directive provides as follows:

The National Security Council/Policy Coordinating Committee (PCC) for National Security Telecommunications, chaired by the Department of Defense, under the authority of National Security Directives 1 and 10, assumed the responsibility for the National Security Telecommunications NSDD 97 Steering Group. By authority of this directive, the PCC for National Security Telecommunications is renamed the PCC for National Security Telecommunications and Information Systems, and shall expand its authority to include the responsibilities to protect the government's national security telecommunications and information systems.

#### (Emphasis added).

Thus, by its own terms, NSD 42 "expands" DOD's authority to include "information systems." What is the significance of this new authority? Will it result in military control of systems previously deemed to be civilian?

3. NSD 42 appears to consolidate NSTISSC (The National Security Telecommunications and Information Systems Security Committee) authority for both computer security policy and computer security budget determinations.

According to section 7 of the revised directive, the National Manager for NSTISSC shall:

j. Review and assess annually the national security

telecommunications systems security programs and budgets of Executive department and agencies of the U.S. Government, and recommend alternatives, where appropriate, for the Executive Agent.

NTISSC has never been given budget review authority for federal agencies. This is a power, in the executive branch, that properly resides in the Office of Management and Budget. There is an additional concern that Congress's ability to monitor the activities of federal agencies may be significantly curtailed if this NTISSC, an entity created by presidential directive, is permitted to review agency budgets in the name of national security.

4. NSD 42 appears to weaken the oversight mechanism established by the Computer Security Act. Under the Act, a Computer Systems Security and Privacy Advisory Board was established to identify emerging issues, to inform the Secretary of Commerce, and to report findings to the Congressional Oversight Committees. Sec. 3, 15 U.S.C. Sec. 278g-4(b).

However, according to NSD 42, NSTISSC is established "to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement provisions of this Directive." What is the impact of NSTISSC authority under NSD 42 on the review authority of the Computer Systems Security and Privacy Advisory Board created by the Computer Security Act?

#### Conclusion

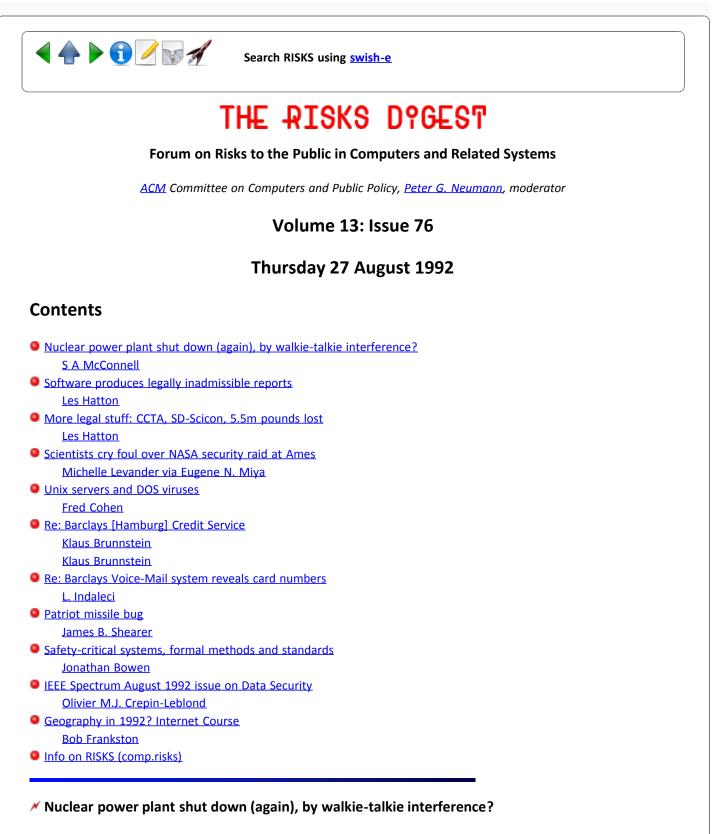
Five years after passage of the Computer Security Act, questions remain about the extent of military involvement in civilian and private sector computer security. The acknowledged role of the National Security Agency in the development of the proposed Digital Signature Standard appears to violate the congressional intent that NIST, and not NSA, be responsible for developing security standards for civilian agencies. The DSS experience suggests that one of the costs of permitting technical standard setting by the Department of Defense is a reduction in communications privacy for the public. The recently released NSD 42 appears to expands DOD's security authority in direct contravention of the intent of the Computer Security Act, again raising questions as to the role of the military in the nation's communications network.

There are also questions that should be pursued regarding the National Security Agency's compliance with the Freedom of Information Act. Given the NSA's increasing presence in the civilian computing world, it is simply unacceptable that it should continue to hide its activities behind a veil of secrecy. As an agency of the federal government, the NSA remains accountable to the public for its activities.

We commend you for opening a public discussion of these important issues and look forward to additional hearings that might address the questions we have raised.

> Sincerely, Marc Rotenberg, Director CPSR Washington Office





"S A McConnell (319) 395-4225" <sam@iberia.cca.cr.rockwell.com> Fri, 21 Aug 1992 08:49:20 CDT

The Gazette in Cedar Rapids reported on Fri Aug. 21, 1992 that:

"Spurious radio signals may again be the culprit in an automatic shutdown of the Palo nuclear power plant" The shutdown occurred on Monday. The Gazette also reported that "A similar incident occurred in June 1989." They believe a security guard walking by a control panel with his walkie-talkie caused the control panel to trigger a shutdown.

I am glad that it did not tell the system to pull the control rods. Why think about microwave ovens being turned on via radio signals when you can talk about nuclear plants being effected by radio signals.

sam@iberia.cca.cr.rockwell.com (S. A. McConnell)

Yes, we have more in Iowa than just corn.

### Software produces legally inadmissible reports

<lesh@prl0.uucp> Fri Aug 21 18:11:15 1992

>From Les Hatton, <lesh@prl0> Programming Research Ltd., U.K.

Software produces legally inadmissible reports: Computer weekly, Thursday, 30 July, 1992.

"Thousands of pounds in poll tax arrears are being left uncollected because of a "design fault" in ICL's Comcis software package. Cash-stricken London councils, including Lambeth and Southwark, have had to delay debt collection after magistrates rejected their computer printouts as evidence. ..... (the bench) ruled that defaulter's debts had to be broken down into individual years and not the single sum given by Comcis, which, as the market leader, is used by about 400 councils.

... Bob Hoskins, head of IT at Southwark commented "Instead of sending out 1,500 summonses per week, we're limited to issuing only 1,000 because of the time it takes to amend the documents manually".

... An ICL spokesman said the authorities affected had only themselves to blame ... "We are not turning our back on these customers and are doing are best to help", he added".

What an extraordinary response by the supplier !

## More legal stuff: CCTA, SD-Scicon, 5.5m pounds lost

<lesh@prl0.uucp> Fri Aug 21 18:11:15 1992

Computer weekly, Thursday 6 Aug, 1992.

"A financial fiasco involving the loss of 5.5m pounds of taxpayer's money has prompted the CCTA, Whitehall's computer adviser, to toughen its contracts with suppliers. ... Last year the roads service of the Dept. of the Environment for Northern Ireland found that although it had paid services company SD-Scicon 5.5m pounds for an IBM 3090 mainframe and software, it did not own the system, and was legally not entitled to use it. The anomaly came to light following a legal dispute between users and SD-Scicon in which solicitors said ownership of the system did not pass to the department until it had been accepted and paid for in full.

SD-Scicon's development was never completed and the system did not undergo acceptance tests, but users in Northern Ireland had paid SD-Scicon 5.5m pounds for the first phases of work - money which was completely wasted.

A Northern Ireland Audit Office report says users had to pay SD-Scicon a further 1.8m pounds on top of the 5.5m pounds to enable the department to own the IBM mainframe they had already paid for. But the IBM software was later scrapped. The department said this week it has now devised a new computing strategy to minimise risk."

A most interesting story. Sell a contract based on hardware and software, don't complete the software and charge extra for use of the hardware the customer had already bought !!

Dr Les Hatton, Director of Research, Programming Research Ltd, England lesh@prl0.co.uk (44) 372-462130

### Scientists cry foul over NASA security raid at Ames

Eugene N. Miya <eugene@nas.nasa.gov> Wed, 19 Aug 92 14:30:49 -0700

Markets \* High Tech \* Economy San Jose Mercury News, Saturday, August 15, 1992 Business section, Pages 9E and 14E

Scientists cry foul over NASA security raid at Ames By Michelle Levander, Mercury News Staff Writer

A security raid that one scientist likened to a "KGB attack" at NASA/Ames Research Center two weeks ago has pitted scientists who depend on the free international exchange of ideas against government bureaucrats afraid of losing economically valuable technology.

On the weekend of July 31, a security force from NASA headquarters in Washington, D.C., descended on research facilities at Ames in Mountain View, changing locks, sending scientists home without explanations, searching through papers on desks and reading people's electronic mail and computer files. The security team, sent by NASA's new administrator, Daniel Goldin, then interrogated some of the most distinguished experts in the country in aeronautics research and temporarily denied about 10 researchers access to offices and computer files.

Harvey Lomax, chief of the Computational Fluid Dynamics Branch at NASA/Ames, said the search -- conducted by men without badges who sent people home or interrogated them without any explanation -- violated the university-like atmosphere he tries to create among his staff. Lomax said he understood the need need to protect security, but, he said, in his 48 years at Ames, "I have never seen an instance of such insulting contempt."

The NASA search was aimed at reviewing the center's handling of classified material and to "review our safeguarding of technologies that are important to national competitiveness," NASA/ Ames director Dale Compton said in a letter to employees this week. Compton apologized in an open letter to NASA scientists for an event that "disrupted" a work culture that "promotes an open exchange of scientific information."

A center spokesman said he knew of no specific incident or security breach that prompted the search but said it was legal for the government to search employees' desks and files.

Now that fears of Cold War enemies have died down, government officials are try to prevent information-sharing between government scientists and their colleagues in other countries that compete with ours. But some critics say such policies could isolate the U.S. scientific community and stymie basic scientific research normally conducted in the international community. [...]

NASA/Ames scientists said they have also recently face increasingly tight restrictions on what information they can share with others and often have to submit work to a government official in Washington for approval. Scientists agree that some research shouldn't be shared but complain that Washington bureaucrats can't tell the difference between basic research and a sensitive technology transfer.

In a meeting with staff this week, Compton said top NASA officials were concerned that ideas on fluid dynamics or other topics could end up in the hands of aerospace or auto companies abroad rather than U.S. firms. "He said we are funded by the United States and one of our missions is to do basic research for industry and not give a competitive edge to others," said one scientist at a meeting held by Compton on the raid.

One irony apparently unnoticed by search team investigators, however, was that while they were taking action against staffers who sent computer transmissions of information abroad, scientists from Germany, France, Spain, Israel and Japan were working on Ames computers and sharing research ideas with their U.S. counterparts as the invited guests of the research center.

The theoretical research done at Ames often involves international collaboration. In fact a good deal of the center's research is published in a British journal.

The research units apparently targeted by the search use supercomputers to solve complex equations governing how a fluid moves, which scientists said is far removed from immediate practical applications. In such theoretical research, involving a single equation can take as much as 500 hours of supercomputer time.

[The article also notes allegations of racism from the Asian-American Pacific Islander Advisory Group at Ames, and strong denials from Ames. PGN]

✓ Unix servers and DOS viruses

## Mr Fred Cohen <cohen@fitmail.fit.qut.edu.au> Sat, 22 Aug 92 15:01:05 EST

Well, it's worse than I thought it would be. Unix experiments through last night showed that viruses succeeded in infecting files that didn't have read or write access. I could even run programs with no read, write, or execute privileges! It seems that the Unix networking allows far more than the access controls permit to the local Unix user. Directory protection seemed to work right, but then, I was able to load and execute files from directories with only Execute permission - not a good sign.

I got a lot of mail about the last posting. I don't think I'm a moron, and if someone can break Novell in 2 days, I don't think the situation gets better by spending more time. Novell version 3.11 - I used the default installation with no 3rd party software - I do know the difference between file attributes and directory rights, and the inheritence does indeed work the opposite of the way the manual describes it. I am replacing the renowned virus marketing expert John McAfee at the Vbull conference - first speaker on the first day - I think. Full details of the experiments will be published at that conference, and after we get some more experiments done, I hope to submit to Computers and Security. Perhaps some of you should read the paper before making assumptions and calling me names. In anticipation of more questions about Unix, System V3.2 with Sun's PC/NFS on the PCs. Default installation - I still don't think I'm a moron - No I haven't tried setting the file system to Read-Only, I am only looking at how an average network might be installed by an average administrator, not at how the world's leading expert on Novell might do it after spending a year to get it right. Want to repeat the experiment? I think the paper provides adequate documentation to allow a thorough repetition, and we repeated the test with independent people watching to make sure we weren't doing something wrong. By the way, the peron installing the Novell has done a number of commercial installations before, and to claim that they know nothing about how to make Novell safe is confirmation of the fact that it is hard to understand the way inheritance, rights, and attributes work together, and that many Novell installations may be unsafe. I doubt if any legitimate and knowledgeable people from Novell will disagree with my findings once they come to the conference and/or read the paper.

Which brings me to one last point. I got a lot of complaints, but only one person wanted to perform similar experiments to confirm our results. There is a big risk associated with unconfirmed (or refuted) results. I don't believe all I read either, but if I really want to know, I repeat the experiment or ask for more details.

FC

## Ke: Barclays [Hamburg] Credit Service misused

<brunnstein@rz.informatik.uni-hamburg.dbp.de> 20 Aug 92 20:46 +0100

In Risk Forum Vol.13, Nr.74, Adrian Howard summarizes a report in UKs (quality) newspaper Independent about a hacker attack on Barlays (Hamburg) Credit Card Service. The original article to report the fact (which was also mentioned in

German TV, 1st channel, on Sunday August 16, 1992) appeared in the weekly magazine "Der SPIEGEL" (also regarded as quality press product) which had issued a press release on Sunday (marketing).

Having been asked on Sunday (immediately after returning from a sailing trip) for some comment (for another publication), I preferred to analysed the case myself in more detail. My findings regarding the facts are less spectacular (though some information holes may never be filled), but now I understand why "Der SPIEGEL" blew up this story (see background).

The facts: Barclays Credit Card Service offers advice via a published 130-number (tool-free, equivalent to 800 in USA). During non-office hours, to record questions and messages of customers, Barclays has a computerized telephone call recorder, using a Meridian system of Northern Telecom.

Incoming calls are recorded on the system's store in sequential order. According to "Der SPIEGEL", messages of the following kind were recorded:

message #3 (date/time recorded): person NN1 asks to increase the credit limit from 3.5 kDM to 8 kDM;

message #7 (date/time recorded): person NN2 reports that his new card with given number and account had arrived.

The Meridian system enables remote invocation of the stored invocation of the stored information, as many telephone call recorders do. In this case, a special combination of telephone keys plus a 3-digit code enables to listen to the recorded voice mail from any telephone (but using the same technique which hand-held devices for remote operation of telephone recorders use).

According to Der SPIEGEL, "888" was used as secret code; Barclays responsible manager (a marketing expert) denied that but admitted that only a 3-digit key was used.

Der SPIEGEL describes the potential misuse of credit cards in some detail. Indeed, knowledge of credit card numbers, accounts and expiration dates allow misuse in telephone trade etc.

Analysis: A1)Without doubt, Meridian is computerized equipment which moreover can be directly connected to work stations and mainframes for automatic processing. Barclays regarded this as "merely a telephone recorder" even when I spoke to them (they argued that this is not a Computer Security problem so I should not be interested!) Unfortunately, as no personal data files in the normal sense are stored, the German national and the Hamburg state Data Protection legislation do not apply; therefore, Hamburg Data Protection ombudsman Dr.Schrader's reaction ("unresponsible") behaviour as mentioned by Adrian Howard was not justified by legal evidence.

A2) As the Meridian system allows for significantly longer authentication code (at least 6 digits, while Barclays used only 3), and as the feature to automatically enforce a new code after a given period was not used by Barclays, they used the digital message recorder not in the safe way which the nature of the customer information deserved. Only after the journalist's recherche, they are now reconsidering this problem. A3) The responsible manager said that NO connection to their mainframe was installed. After some discussion with him and some contradicting information, some doubts remain. He told me that a major revision of the system's use is underway (and that his experts do not have time to answer my few questions) but when merely used as telephone recorder, improvements are easy and fast to install (as Northern Telecom specialists worked there).

In the SPIEGEL report, there is no evidence for a break-in into Barclays mainframe but their denial to allow me to see the system with several, partially contradicting reasons given at times leaves some doubt (background: I supervise the largest European backup center for banks, insurances etc, with a 300 MIpS/1.0 TByte machine and inspect large computer centers on a regular basis).

A4) In the last part of SPIEGEL's article, there are several references to Kimble's case (see my corresponding report in July) who demonstrated a new phreaking technique to the German economic monthly "CAPITAL" (and a German TV station). Presently, some research "from a Cologne as well as from a Californian security advisory enterprise" are underway, according to Der SPIEGEL, and in these cases, "computer kids .. received significant honoraries". There is indeed evidence that competing hacker and phreak groups (esp. Kimble with CAPITAL versus Chaos Club which was cited as information source by Der SPIEGEL) seem to entertain a showdown for honoraries. Kimble, in several (paid) interviews, made some negative comments on Chaos Club. As CCC explicitly (citations) and implicitly (some undocumented role in the phreak action) is connected with this case, it is not improbable (to be cautious) that this phreak attack was one reaction to the Kimble case. It is interesting to remember that several Hamburg journalists (then at a TV station, one of which works since some time for SPIEGEL) first reported Chaos Club's NASA and KGB activities.

Summary: The report of SPIEGEL (and those derived from it) concerned a phreak attack on a digital telephone recorder; the presentation of the facts and esp. implications for a bank computer attack were inadequate. The attacked bank demonstrated a shockingly insufficient knowledge of security demands and procedures related to a new digitized service.

Klaus Brunnstein, University of Hamburg (August 20, 1992 8:15 pm)

### vpdate: Barclay voice mail insecurity

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
27 Aug 92 16:16 +0100

Update of Barclay Hamburg Credit Card Service's Voice Mail insecurity:

The evident contradiction between Meridian Mail's minimum keynumber length (4..16 digits) and the fact that a 3-digit code was used found a surprising explanation: Northern Telecom requires for the US/Canada product \*at least 4 digits code\*, whereas the German version was reduced to require \*at least 3 digits\*. This has possibly to do with the fact that most European customers have smaller telephone systems with less than 999 lines connected. After this

incident, Northern Telecom Europe decided to improve European applications to US/Canada standards, requiring 4..16 Bytes. Moreover, they will put more emphasis on enfording regular changes of keynumbers.

According to Northern Telecom experts, Barclay connected a WYSE terminal for service purposes via RS 232 port; the general software needed to connect the Meridian Mail system to another computer (sw Meridian Link) was not installed, said NT officials. This implies that the surprisingly long time needed for security improvement (more than one week of several experts, including NT personnel) was needed to upgrade the knowledge of the "experts". As security improvements are really simple (about 1 hour), serious doubts remain (even assuming maximum incompetence of Barclay Hamburg "experts").

The Hamburg Data Protection Ombudsman presently examines the case; he assumes that the digitized system has a file of personal data which entries may be individually retrieved, such that Data Protection laws apply. There is some doubt that the legal definition may apply to a flat file of characters without any ordering structure and no retrieval functions available in the system.

Klaus Brunnstein (Univ of Hamburg, August 27, 1992)

## Ke: Barclays Voice-Mail system reveals card numbers [RISKS-13.76]

<amadeus@flex.com> Sun, 23 Aug 92 18:10:16 -0400

I discovered a situation very similar to the Barclays voice-mail incident, right here in the US.

Sometime a couple years ago my roommate received a letter from a company called TeleCredit regarding his Visa charge card that was issued to him by a small local bank. Apparently, TeleCredit was contracted by the small local bank to handle the issuing and billing matters of the credit cards that the local bank was offering.

The letter requested that my roommate call a 800 number and with a touch-tone phone enter a certain extension and leave his account number and name and a short statement that they did receive their card in a recording. I found this very interesting and gave their voice-mail system a call.

Since I am a hacker, I instinctively pressed the # key followed by the voice mail box number to enter the mail box, and found to my surprise that there was no password protecting the messages people were leaving! I wasn't as surprised as others might be since as a seasoned hacker I knew this kind of situation was all too common.

For [a?] month I called the voice mail box and listened to about 30 messages a day of people leaving their names and credit card numbers and SSN numbers and daytime phone numbers. Unlike the letter, the greeting to the voice mail box requested they leave such info. Being inside the voice mail box could have even allowed me to change the greeting to ask for other sensitive info, and common folks not knowing any better would have left it with no hesitation. Of

course, I did no such thing. If I were malicious, I might even change the password and TeleCredit, not knowing how to set a password, would have taken a few weeks to figure out how to change it back and thus would have a major interruption in their card accounting procedure.

I suspect a similar thing happened with the CCC and Barclays, and all Barclays need do is read their voice mail system manuals. No need to hire CCC to come in and explain it for them. All CCC has to say is rtm (read the [...] manual). I wonder if I had broken my little discovery to the press it would have become the media circus the CCC is always striving for. I can see the headlines now: "Hacker Cracks Credit Card Database; Privacy of Thousands of Accounts In His Hands!"

Luckily, TeleCredit wised up after about six months and has apparently discontinued the practice of having customers report their account numbers to a voice mail-box, for the mail-box was discontinued. However, other less sensitive mailboxes still lie wide open.

I still have recordings on tape of the messages people were leaving on that TeleCredit mailbox that I forgot about, the Barclay article made me remember that I had still had them.

Amadeus

[ADDED NOTE: The system flex.com has cut its UUCP feed do to financial considerations, so any mail to that account would have bounced (as it would now). You can reach me at indaleci@uhunix.uhcc.hawaii.edu, courtesy of a friend. Thank You, Amadeus]

### 🗡 Patriot missile bug

<jbs@watson.ibm.com> Thu, 20 Aug 92 14:05:35 EDT

An article in the July 1992 Siam News by Robert Skeel contains more information on the Patriot missile bug. Apparently the program contained representations of .1 as both 24-bit and 48-bit fixed point binary numbers. If either had been used consistently there would have been no problem. However using both proved disastrous as it introduced errors of the form (.1d-.1e)\*t (where .1d is the 48 bit representation, .1e is the 24 bit representation and t is the time elapsed since the clock was zeroed). I got the impression that the software was written in a pretty slipshod way.

James B. Shearer

### Safety-critical systems, formal methods and standards

<Jonathan.Bowen@prg.ox.ac.uk> Tue, 25 Aug 92 18:14:06 BST

Readers of risks may be interested in a one-page article in the August issue of BYTE magazine by Richard Stein entitled "Safety by Formal Design" (p157). This article cites the Therac 25 accident and the possibility of using formal methods to help prevent such accidents in the future.

I first learned about this article when our librarian started to receive many requests for a Technical Report on "Safety-Critical Systems, Formal Methods and Standards" (PRG-TR-5-92) by me and Victoria Stavridou which is referenced in the article. This report was compiled from a wide range of sources, including a request for information on RISKS. Because there seems to be considerable interest in the report, I am making it available via FTP to save some of our mailing costs to those on Internet with FTP access and a PostScript printer. If you wish to obtain the report, use anonymous FTP to "ftp.comlab.ox.ac.uk" (192.76.25.2), change directory to "Documents/techreports" and get the PostScript file "TR-5-92.ps". If you do not have FTP access, you can obtain a paper copy by sending your name and address to our librarian on library@comlab.ox.ac.uk>.

<Jonathan.Bowen@comlab.ox.ac.uk>
Jonathan Bowen, Oxford University Computing Laboratory

### IEEE Spectrum August 1992 issue on Data Security

"Olivier M.J. Crepin-Leblond" <ocl@cc.imperial.ac.uk> Thu, 27 Aug 1992 23:11:22 +0100

I thought I'd mention that the IEEE Spectrum Magazine, August 1992 issue, is all about Data Security. And one of the articles, `A security roundtable' includes an artist's view of our moderator, Peter G. Neumann ! A bonus article is concerned with reliability and MIL-HDBK-217, long the bible of the U.S. defense industry. All in all, pretty interesting reading, recommended to all RISKS readers !

Olivier M.J. Crepin-Leblond, Digital Comms. Section, Elec. Eng. Department Imperial College of Science, Technology and Medicine, London SW7 2BT, UK

### ✓ Geography in 1992? Internet Course

<Bob\_Frankston@frankston.com> Wed 26 Aug 1992 17:38 -0400

In fact, this is an appropriate subject for a geography course. But I still find the placement in that department as an interesting development.

From: abw@bucrsb.bu.edu @ uucp Date: 08-26-92 14:56:10 EDT (08-26-92 15:16:29 EDT) Subject: Internet courses

Is there any place around here where an actual COURSE on the Internet is taught? At MIT, or any of the other schools, or anywhere?

Boston University is offering the following this Fall. ---Al

>From sam@bu-it.bu.edu Mon Apr 1 05:05:46 1992 Subject: New Geography course offered this fall.

## COMPUTER NETWORKS AND SOCIAL NETWORKS IN DEVELOPING COUNTRIES (GG 792)

Prof. Sheldon Annis Fall 1992 Geography Department Thursday, 3:30-6:30 467 Stone Science Bldg, Classroom: TBA 3-5742 (tel); annis@bucrsb (email)

Computer networks, such as the Internet, are beginning to penetrate Eastern Europe, the Commonwealth of Independent States, Africa, Asia, and Latin America. As a result, students at BU have access to vast new information resources and can now communicate electronically with researchers around the world. This course explores the implications of this new connectivity and teaches students to use these powerful new research tools.

Substantively, the course examines how new information and network technology is affecting people in developing countries. The evolution of networks, their political and economic consequences, and issues in informatics policy will be discussed. Case material will be drawn from Central America, the Philippines, and Africa. Special attention will be paid to World Bank lending in developing countries. Computer networks, GIS, and satellite communication technology (e.g., VitaSat and SatelLife) will be explored.

Students will learn to use networks based on Internet, BITNET, UUCP, and Fidonet technology. (Fidonet is especially important in Africa.) Students can expect to access a wide variety of overseas networks, and should be able to contact researchers in most countries. They will learn basic skills such as the exchange of e-mail, conferencing, and FTP (electronic transfer of documents), as well more advanced skills such as remote searching of library catalogs, use of electronic data bases, access to electronic journals, use of newsgroups, and interactive ("real-time") conversation over the Internet. They will also be introduced to a highly advanced generation of new software -sometimes called "knowledge robots", or "knowbots" -- which can search for information across and through vast, decentralized networks (also called Wide-Area Information Servers).

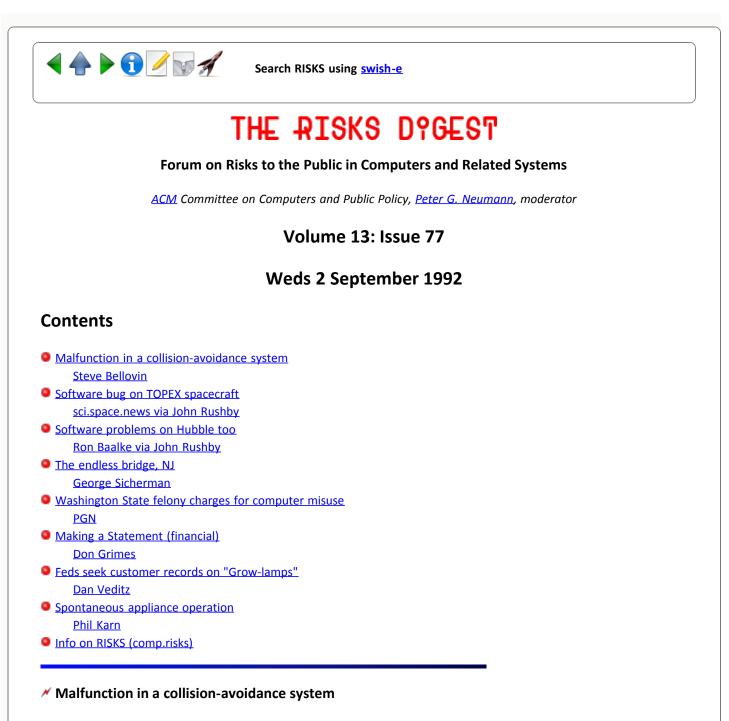
\_Prerequisites and limitations\_: This course is intended for graduate students with well-developed research interest in developing countries \_or\_ students with strong technical backgrounds who want to explore the applications of network technology. Some knowledge of computers is assumed, though not necessarily of networks. Limited to 15 students.

\_Texts\_: \_Zen and the Art of the Internet\_ by Brendan P. Kehoe, and readings on developing countries.

Note: this course is not yet listed in the current Schedule of Classes\_, but it \_is\_ being offered.



Report problems with the web pages to the maintainer



<smb@ulysses.att.com> Tue, 01 Sep 92 15:15:11 EDT

According to the AP, a ``Traffic Alert and Collision Avoidance System'', designed to prevent mid-air collisions, apparently malfunctioned and nearly caused one. Two planes, a 767 and a DC-9, were separated by 1,000 feet of altitude, in accordance with FAA regulations. But the TACAS system told the pilot of the 767 to descend to the DC-9's altitude. The horizontal separation of the planes was only .5 miles, rather than the 5 miles required.

--Steve Bellovin

# Software bug on TOPEX spacecraft (From sci.space.news)

John Rushby <RUSHBY@csl.sri.com> Sat 29 Aug 92 17:20:45-PDT

## TOPEX/POSEIDON STATUS REPORT August 28, 1992

The TOPEX spacecraft went into safemode at 18:13Z on August 27. The project reports that during a planned maneuver that they received a "roll momentum wheel saturated" alarm causing the spacecraft to go into safemode and causing the project to abort the maneuver after 98% completion. The project has elected to remain with TDRS support for the time being. The project has not declared a spacecraft emergency. The cause of the safemode is currently under investigation.

Forwarded from: PUBLIC INFORMATION OFFICE, JET PROPULSION LABORATORY, CALIFORNIA INSTITUTE OF TECHNOLOGY, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, PASADENA, CALIF. 91109. (818) 354-5011

## TOPEX/POSEIDON STATUS REPORT August 28, 1992

The TOPEX/Poseidon satellite entered into safe hold mode on Aug. 27, 1992 at approximately 11:13 a.m. PDT. This incident occurred during the inclination maneuver about 6 seconds from the end of the propulsion burn.

The inclination maneuver was successful and placed the satellite in the proper 66 degree inclination toward the Earth.

Project managers have determined that the safe hold mode was the result of a "bug" in the software code which set the failure detection correction limit for a roll angle of 3 degrees, not 7 degrees as intended. This was a result of residual LANDSAT code which did not correlate to the program design language.

All satellite hardware is functioning properly based on detailed review of the maneuver playback data. Reconfiguration of the satellite back to the standard configuration prior to safe hold mode is in process at this time and is expected to be completed tonight.

The solar array was offset to -55 degrees at 12:45 p.m. PDT today prior to the start of occultation. This was done so as to not overcharge the batteries when the Sun hits the solar array after coming from eclipse.

Since the inclination maneuver goals were achieved, the flight team is proceeding with the nominal maneuver campaign. There are four more maneuvers to go. In-Plane Maneuver One is planned for Wednesday, Sept. 2, 1992.

The NASA radar altimeter was turned off when the

satellite entered the safe hold mode. It will be turned back on about 6:30 p.m. PDT tonight. Initial data from the NASA altimeter prior to the incident looked very good.

### Software problems on Hubble too

John Rushby <RUSHBY@csl.sri.com> Tue 1 Sep 92 19:44:23-PDT

> HUBBLE STATUS REPORT August 31, 1992

HUBBLE SPACE TELESCOPE (HST): HST operations have returned to normal following the recent safehold entry and recovery. Starting on July 30, a chain of events caused HST first to enter an inertial hold safemode followed by a hardware sunpoint safemode. The first was caused by an incorrect ephemeris table that was loaded into the spacecraft computer, and the latter by a problem with an onboard computer software macro. Science observations that were scheduled for execution during the safemode events are being rescheduled. HST launched April 24, 1990 aboard the Space Shuttle Discovery.

Ron Baalke, Jet Propulsion Lab, M/S 525-3684 Telos, Pasadena, CA 91109 baalke@kelvin.jpl.nasa.gov

### the endless bridge

George Sicherman <gls@windmill.att.com> Sun, 30 Aug 92 11:32:25 edt

From the Asbury Park Press, August 30, 1992:

A malfunction in the computer that opens and closes the Route 37 bridge rendered the span impassable for an hour yesterday afternoon, backing up traffic for miles in each direction.

Dover police Sgt. Vincent Pedalino said officers were forced to reroute traffic north to the Mantoloking Bridge on Route 528 while state Department of Transportation workers found a way to repair the computer.

The bridge was closed between 2:30 and 3:30 p.m., stranding many motorists on the bridge in the hot afternoon sun.

Pedalino said the drawbridge structure itself -- which opens upward to allow water traffic through in Barnegat Bay -- was unimpaired, but the automobile barriers wouldn't reopen. Normally there are manual controls that override the computer system, but they also were not working, he said.

The bridge is a long span from the Toms River area to the barrier resort of Seaside Heights and the popular Island Beach. The Mantoloking Bridge is the nearest other exit from the barrier peninsula, about 10 kilometers north. The story does not tell what was wrong with the computer or the manual controls. I wonder whether those "manual" controls would work during a power failure!

Col. G. L. Sicherman, gls@windmill.ATT.COM

### Washington State felony charges for computer misuse

"Peter G. Neumann" <neumann@csl.sri.com> 21 Aug 1992 15:43:08 -0800

An article by O. Casey Corr, The Seattle Times Knight-Ridder/Tribune Business News, 20 Aug 1992, describes the case of Mel Creamer, coordinator of a software system for mainframe computers used in Olympia, Washington, by the Department of Social and Health Services. He was doing a routine check of the system's performance when the following message showed up:

#### "THAT DEVICE DOES NOT EXIST ON STATION DEFINED."

A keystroke-capture watch was set up. It then was determined that this message had been triggered by a temporary clerk-typist trying to print something locally using the access code of another user normally in a different area, and the system could not interpret the command. He was trying to print the file of personal sign-on codes, and had created new accounts and access codes, and had erased audit trails to remove evidence of the activities. He clearly had all the necessary access codes.

The computers contained software for issuing checks and ordering state services, personnel records for the department's 16,000 employees, arrest warrants for parking tickets kept for the Department of Licensing, and private information on individuals and countless companies that did business with the state. A computer linked to the one breached by the intruder maintains the state's budget records. Malicious misuse of those systems could be quite damaging.

Timothy M. Lewis was charged by King County for computer trespass in the first degree, a felony, along with three other people, for misuse dating back to 1987. The victims, in addition to the state, included Aldus of Seattle, Asymetrix of Bellevue, and Phonelink Inc. of Bellevue (now Fox Communications). (This is reportedly something like the 14th such case involving adults since 1988.)

Eugene Raddatz, a data security analyst with DSHS, recalled two previous cases in the 1980s when state employees got into the computer system and stole money by having checks written to themselves. Both people received prison terms, he said.

### Making a Statement (financial)

Don Grimes via gafter@mri.com <deg@mri.com>

### Tue, 25 Aug 92 10:04:04 PDT

For more than a decade I've been a customer of a money-market fund that shall remain nameless here. For all that time, they've sent me a statement monthly. Early on, they returned canceled checks with each statement; some years back they started batching the checks, returning them only twice a year, to save on postage.

In recent months, they've started sending me a statement every time there's activity in my account: every time a check clears, or I make a deposit. In my case, that means a minimum of three statements per month, at 27 cents postage each. So I called up, endured their voicemail system and a five-minute hold, and asked the customer-service person what's going on.

It seems they've just "enhanced" (her term) their computer system, and one of its "features" now is that it kicks out a statement every time there's activity, whether you want one or not. I pointed out that this is costing ten times what they're saving by batching canceled checks, but there's nothing to be done: that's how the computer works, and it can't be changed ...

## \* Feds seek customer records on "Grow-lamps"

Dan Veditz <daniel@borland.com> Fri, 21 Aug 92 11:53:07 PDT

An AP story in today's paper (21 Aug 1992) date-lined San Francisco states that Federal prosecutors sought court orders yesterday to force three local businesses to turn over their customer lists, sales receipts and shipping records for indoor "Growing lights" since the start of 1990. They also want copies of any correspondence mentioning marijuana.

The three companies--Diamond Lights, General Hydroponics, and Berkeley Indoor Garden Center--refused to turn over the documents without a court order and are now fighting the court order on the grounds that the request was too broad and would violate customer privacy.

>From their names I'd guess these businesses sell lots of "grow-lamps"; the RISK is that with the increasing use of sales-registers that record customer identification along with each sale how long until the government starts investigating people who innocently buy a few of these lamps from the local K-mart, or any other item that might just possibly be used in some sort of illegal activity?

-Dan Veditz

### Spontaneous appliance operation

Phil Karn <karn@servo.Qualcomm.COM> Fri, 21 Aug 92 23:55:04 -0700

There's a known problem with the BSR X-10 home automation system whereby the "appliance modules" can spontaneously turn themselves on. This happens with

certain types of loads, particularly electronic loads such as computers and compact fluorescent lights, and it is due to a misfeature called "local on". (The X-10 is a carrier current appliance control system widely marketed under other names, including Radio Shack, Heath and Stanley. The "appliance modules" are relay boxes that plug into the wall between the AC line and a load to be controlled.)

The "local-on" feature is intended to allow a user to turn on an appliance locally, without having to go to the control box. If the appliance is a lamp, you just flick its regular switch on and off several times, and the appliance module turns on.

This feature apparently works by trickling a small amount of current through the load whenever the appliance module relay is 'off' and watching for sudden voltage swings across the load that would indicate that the user is cycling the power switch. It works great for simple resistive loads like incandescent lamps, but nonlinear electronic loads (especially those that directly rectify and filter the AC power line) will often draw almost no current until some voltage is reached across the load's internal filter capacitor. Then the load conducts, discharging the capacitor and causing the input voltage to drop suddenly. A few cycles of this "relaxation oscillator" simulates a user flicking a switch well enough to trigger the appliance module's "local on" feature.

The problem usually occurs right after you switch the load off -- several seconds later, it comes back on again. But it's possible that the spurious turn-on could occur much later. This problem drove me crazy until I realized from the description of "local on" in the manual what was going on. There was no specific warning about this possibility. Indeed, the manuals take great pains to point out that "lamp modules" (which contain dimmers) are not to be used with flourescent lamps and electronic loads; appliance modules should be used instead. The instructions do warn about controlling appliances that could cause damage if they were turned on inadvertently (e.g., an empty coffee pot) but this doesn't really address the issue.

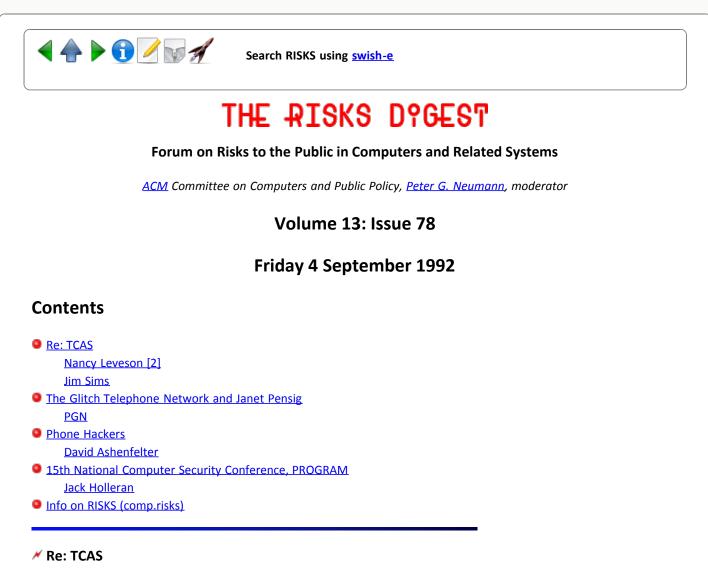
It turns out that cutting an undocumented jumper inside the appliance module defeats the "local on" misfeature. It's obvious that someone anticipated this problem since the jumper wasn't essential in the PC board layout, so it's doubly annoying that there is no mention of this problem or its solution in the manual.

Phil



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Wed, 02 Sep 92 17:53:31 -0700

According to a report that was just on CNN, the problem was that the pilot went the wrong way, i.e, TCAS told him to go up and he went down. In the report (which was surprisingly good) they also mentioned that the controllers hate TCAS because they lose control and that the pilots love it because they gain control. The people interviewed on the report that appeared disturbed by the incident were controllers so it is difficult to really know how serious it actually was.

Nancy

## 🗡 Re: TCAS

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Fri, 04 Sep 92 10:35:07 -0700

Steve Bellovin writes:

According to the AP, a ``Traffic Alert and Collision Avoidance System'', designed to prevent mid-air collisions, apparently malfunctioned and nearly

caused one. Two planes, a 767 and a DC-9, were separated by 1,000 feet of altitude, in accordance with FAA regulations. But the TACAS system told the pilot of the 767 to descend to the DC-9's altitude. The horizontal separation of the planes was only .5 miles, rather than the 5 miles required.

This message is incorrect. There was a good report on CNN, and I also spoke to a friend at the FAA. The pilot sighted the other plane visually before the TCAS alert and mistakenly thought the plane was at the same altitude. He descended. From everything the FAA can determine, TCAS gave a correct advisory and did not "malfunction." The pilot says that he does not remember what the TCAS advisory was but that his maneuver came before the advisory and was based on his visual sighting.

If you read about TCAS, you need to be aware that it is in the midst of a big political struggle. The pilots love it (there was a representative from ALPA on the CNN report). The controllers hate it. According to my friend in the TCAS office at the FAA, the data released by the controller's union about TCAS problems and printed in some newspaper reports of this recent incident is just not correct. So watch who is speaking when you hear about TCAS and its problems or advantages.

In case there is anyone who doesn't know, my Ph.D. students (Mats Heimdahl, Holly Hildreth, Jon Reese, Ruben Ortega, and Clark Turner) and I are working on a formal system requirements specification of TCAS II. This will serve as the official FAA specification of TCAS and also as a testbed application for their dissertations on safety analysis and risk assessment.

Nancy Leveson

## 🗡 TCAS

Jim Sims <sims@drake.mitre.org> Thu, 3 Sep 1992 14:09:44 GMT

In the version of the TCAS story I saw locally about the 2 USair jets near-miss, it mentioned that for the period june -June of the previous year, over 60% of the warnings/advisements from TCAS systems nationwide have been erroneous. Many of these have been of the same sort reported -- the system told two planes that were "safe" to maneuver into an "unsafe" flight path....

sims@starbase.mitre.org The MITRE Corporation, 7525 Colshire Drive, MS Z421, McLean, Va. 22102 DECUS AI SIG Symposium Representative

### M The Glitch Telephone Network

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 4 Sep 92 10:39:49 PDT

The current issue of The New Yorker (7 Sept 1992) has an item in The Talk of the Town on the Glitch telephone network. Call 212-228-7514 and get a "glaring light each week on some dark alley that science is currently leading us down.

In the past several months, Glitch has alerted us to the hazards of computer technology, the vulnerability of telephone privacy, and the folly of the high-speed chase."

I called Janet Pensig, who runs this line. Her message of the week deals with polymorphic viruses. She also notes that The New Yorker fabricated all sorts of quotes and missed the content of what she was saying. She is said by the article to be "deeply pessimistic about the future", which she says on the tape is not at all what she told them! I left her a message, and when she called me back I discovered that she has been faithfully reading the RISKS section of the ACM Software Engineering Notes, as well as Inside Risks in the CACM. She is very serious about what she is doing. This seems like a wonderful educational opportunity for new yorkers (lower case to distinguish them from the magazine).

The Talk of the Town writer ended the last paragraph of the item like this: "We knew that ... we would never know the true face of doom -- so we just thanked her for her time and told her that we now felt much worse."

Check out Glitch if you wish. PGN

[The NYer item was called to my attention by John Rushby, who got to his issue before I got to mine...]

## Phone Hackers

"Peter G. Neumann" <neumann@csl.sri.com> 2 Sep 1992 15:47:25 -0800

By David Ashenfelter, Detroit Free Press Knight-Ridder/Tribune Business News

DETROIT--Sept. 1--In the late 1980s, high-tech pranksters got their kicks by breaking into unprotected computer systems. Then, they infected computers with harmful binary viruses. Today, hackers are wreaking havoc on computerized telephone systems. "It's a big problem and getting worse," said John Haugh, a Portland, Ore., a telecommunications expert who estimated that hackers are responsible for about \$4 billion a year in toll fraud. "Once they get inside the system and get a dial tone, they can make phone calls all over the world," Haugh added. "By the time the customer gets his phone bill, the criminals are long gone."

The Detroit Newspaper Agency (DNA), publisher of the Detroit News and Detroit Free Press, recently became a victim of one variation of the telescam. Three months ago, DNA employees started finding strange messages in the company's computerized voice mail system. The messages were intended for someone else and were left by callers who identified themselves as "Black Lightning," "Phantom," or "Plastic Man." What initially appeared to be a glitch in the voice mail system turned out to be the work of a hacker who broke into the message system through a dial-in maintenance line, said DNA telecommunications manager Ricardo Vasquez. Once inside, the hacker cracked the system administrator's pass code and set up scores of voice mailboxes for friends and associates who dialed in on the DNA's toll-free number. Later, officials at Shell Oil Co. in Houston and Shearson Lehman Bros. in St. Louis notified Vasquez that their voice mail systems had been penetrated by hackers who left messages urging their friends to call a mailbox at the DNA. "We were lucky," Vasquez said. "Our losses amounted to only a few hundred dollars for calls on our toll-free phone line." He said the company's losses would have been far worse had the system been equipped to allow the intruders to make worldwide long-distance calls on DNA phone lines. Vasquez said the DNA does not plan to request a criminal investigation because losses were small.

Officials at Shell Oil and Shearson Lehman declined to comment. Michigan Bell security employees referred inquiries to the public relations staff, which, in turn, referred inquiries to the Tigon Corp., an Ameritech subsidiary in Dallas which sells and leases voice mail systems. "It is a growing problem and people need to be aware of it," said Tigon spokesperson Jill Boeschenstein. "In most cases, hackers try to get in to have some fun and fool around with the message system. "The real expense comes when they're able to make outgoing calls that the company ends up paying for. That can be a considerable sum before company realizes what is going on." Boeschenstein said companies that buy or lease voice mail systems are responsible for unauthorized usage. She said companies can protect their phone systems relatively easily by using longer pass codes and disconnecting maintenance phone lines which enable system administrators to operate the system from a remote location. Boeschenstein also said companies should do a more thorough job of monitoring their systems.

Telecommunications expert Haugh, whose company interviewed more than 400 toll-fraud victims or near victims, said the most sinister telephone hackers break into a phone system and set up hidden mailboxes, then sell them to drug, prostitution and child pornography rings that want to make free calls that are hard to trace.

Hackers also market mailboxes to nationwide rings which sell long-distance phone calls for \$10-\$30 apiece from pay phones on the streets of large U.S. cities. Haugh said many of the customers are immigrants who want to call relatives in their homelands.

A favorite time for hackers to sell phone service is on weekends when companies aren't using or monitoring their phone systems, some of which are capable of handling hundreds of long-distance calls simultaneously. Haugh said one nationally-known manufacturer which he declined to identify belatedly discovered that it was on the hook for \$1.4 million worth of long distance calls made on its phone lines in just one weekend. And after companies are victimized, they rarely are willing to discuss it publicly. "They're afraid of bad publicity or liability and in almost all cases their fears are unfounded," Haugh said. "It's a very foolish attitude. Until the problem becomes better understood, other companies aren't going to do enough to protect their systems from abuse."

### 15th National Computer Security Conference, PROGRAM

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL> Fri, 4 Sep 92 16:40 EDT Tuesday October 13 10:00a.m., Hall E, OPENING PLENARY Welcome: Mayor Kurt L. Schmoke, Baltimore City (invited) James H. Burrows and Patrick R. Gallagher, Jr. Keynote Speaker: Roland Huber, Commission of the European Communities Systems Security Award Ceremony Best Paper Awards Wednesday October 14 CONFERENCE BANQUET (7:00p.m.) Speaker: Dr. Peter G. Neumann, SRI International Computer Security and Human Insecurity Thursday October 15

Registration Information: Tammie Grice (301) 975-2775

Conference Awards Reception (6:00p.m.)

Friday October 16, 11:00a.m., Room 307 - 308 - 309 CLOSING PLENARY E. Troy, Chair, NIST Panel Discussion International Standards: A Path to International Harmonization Panelists: D. Herson,United Kingdom ; S. Knapskog, ISO/SC27/WG3; U. Van Essen, Germany; R. Verrett, Canada

Technical Program 2:00p.m. Hall E Panel - Criteria I: Perspectives and Progress on International Criteria E. Troy, Chair, NIST "The IT Security Evaluation Manual" Y. Klein, Service Central de la Securite des Systemes d'Information, Paris, France Panelists: LTC R. Ross, NSA; D. Ferraiolo, NIST; E. Bacic, Canada; J. Wood, European Communities

Room 309 Covert Channels, Part I: Analysis Dr. B. Burnham, Chair, NSA "Architectural Implications of Covert Channels" N. Proctor and P.G. Neumann, SRI International "A Foundation for Covert Channel Analysis" T. Fine, Secure Computing Corporation "A Tool for Covert Storage Channel Analysis of the UNIX Kernel" D. Willcox, Motorola Microcomputer Group Room 307-308

Panel: The TPEP and Product Innovation R. Henning, Chair, Harris Corporation; Panelists: Room 319-321

J.Adams, SecureWare; L. Baron, Sun Microsystems; W. Boebert, Secure Computing Corporation; Dr. M. Branstad, Trusted Information Systems, Inc.; Dr. R. Schell, Gemini Computers

Room 301-303 Threats and Security Overview LtCdr. A. Liddle, Royal Navy, National Defense University

Panel: Virus I: Virus Attacks & Counterattacks - Real-World Experiences J. Litchko, Chair, Trusted Information Systems, Inc. Panelists: L. Mandeville, Miller, Belis & O'Neil, P.C.; J. Keyes, NASA; G. Wellham, Maryland National Financial, Inc. **Room 305** New Security Paradigms (Part I) 2:00-5:30p.m. H. Hosmer, Chair, Data Security, Inc. "A New Paradigm for Trusted Systems" Dr. D. Denning, Georgetown University Discussion Leader: Dr. L. LaPadula, The Mitre Corporation "New Paradigms for High Assurance Software" Dr. J. McLean, Naval Research Laboratory Discussion Leader: E. Leighninger, Dynamics Research Corporation "Managing Complexity in Secure Networks" Dr. D. Bailey, Galaxy Systems Discussion Leader: Dr. M. Abrams, The Mitre Corporation "Best Paper of the New Security Paradigms Workshop" Discussion Leader: E. Leighninger, Dynamics Research Corporation Panel Discussion Dr. J. Dobson, Newcastle upon Tyne; Dr. D. Bailey, Galaxy Systems; Dr. D. Denning, Georgetown University; H. Hosmer, Data Security, Inc.; Dr. L. LaPadula, The Mitre Corporation; Dr. J. McLean, Naval **Research Laboratory** 4:00p.m. Hall E International Harmonization E. Flahavin, Chair, NIST "Re-Use of Evaluation Results" J. Smith, CESG Panel: TMach as a Symbol of International Harmonization

Panelists:

B. Boesch, DARPA; Dr. M. Branstad, Trusted Information Systems, Inc.; C. Ketley, U.K. Government; K. Keus, German Government

Room 309 Panel - Covert Channels, Part II: Overt Truths Behind Covert Channels P. Neumann, Chair, SRI International Panelists: R. Morris, NSA; J. Millen, The Mitre Corporation; V. Gligor, University of Maryland

Room 307-308 Evolving Security Requirements F. Mayer, Chair, Aerospace Corp. "Extending Our Hardware Base: A Worked Example" N. McAuliffe, Trusted Information Systems, Inc.

"Evolving Criteria for Evaluation: The Challenge for the International Integrator of the 90's" J. Fowler, Grumman Data Systems

"The Need for a Multilevel Secure (MLS) Trusted User Interface" G. Factor, Digital Equipment Corp.

Room 317

Information Technology Security Requirements PanelD. Gilbert, Chair, NISTPanelists:N. Lynch, NIST; S. Pitcher, Department of Commerce; M. Swanson, NIST; Dr. W. Maconochy, NSA

Room 301-303 Physical, Personnel, and Administrative Security H. Looney, National Defense University

Room 319-321 Viruses II: VIRUS Proposed Approaches J. Anderson, Chair, J. P. Anderson Company "Software Forensics: Can We Track Code to its Authors?" Dr. E. Spafford, Purdue University "Precise Identification of Computer Viruses" T. Polk, NIST "Data Security for Personal Computers" P. Bicknell, The MITRE Corporation

October 14 9:00a.m. ROOM 309 DBMS I: Security in Database Management Systems C. Meadows, Chair, Naval Research Lab "Enforcing Entity and Referential Integrity in Multilevel Secure Databases" V. Doshi, The MITRE Corporation "A Multilevel Secure Database Management System Benchmark" L. Schlipper, The MITRE Corporation

"Protected Groups: An Approach to Integrity and Secrecy in an Object-Oriented Database" J. Slack, Kansas State University

"Implications of Monoinstantiation in a Normally Polyinstantiated Multilevel Secure Database" F. Kramer, Digital Equipment Corporation

Room 307-308 Perspectives on MLS System Solution Acquisition - A Debate by the Critical Players Involved

J. Sachs, Chair, ARCA Systems Inc. "An Approach for Multilevel Security (MLS) Acquisition" W. Neugent, The Mitre Corporation Panelists: T. Clarke, Defense Information Systems Agency; A. Cuomo, NSA; G. Evans, Loral Western Development Labs; Col. J. Hackman, USAF, Joint Chiefs of Staff; B. Loiter, Digital Equipment Corporation; H.O. Lubbes, Naval Research Lab; Dr. W. Wilson, Arca Systems Inc. Room 317 Network Security W. H. Murray, Chair, Consultant "Toward a Model of Security for a Network of Computers P. Farrell, George Mason University "Risk Management of Complex Networks R. Cox, CTA "A Local Area Network Security Architecture L. Carnahan, NIST "Priorities for LAN Security: A Case Study of a Federal Agency's LAN Security S. Chang, NIST Room 301-303 **Trusted Systems Concepts** Dr. C. Abzug, National Defense University Room 319-321 Panel - Information Systems Security Organization: Retooling for the Future Dr. W. Maconachy, Chair, NSA Panelists: S. Barnett, NSA; R. Quane, National Cryptologic School; A. Whieldon, NSA Room 305 New Security Paradigms (Part II) 9:00-12:00a.m. Dr. J. Dobson, Chair, Newcastle upon Tyne "The Multipolicy Paradigm" H. Hosmer, Data Security, Inc. Discussion Leader: Dr. T. Haigh, Secure Computing Corporation "Metapolicies II" H. Hosmer, Data Security, Inc. Discussion Leader: Dr. L. LaPadula, The Mitre Corporation "Separation Machines" Dr. J. Graff, Amdahl Discussion Leader: M. Smith, AT&T "Mediation and Separation in Contemporary Information Technology Systems" J. Heaney, The Mitre Corporation Discussion Leader: E. Leighninger, Dynamics Research Corporation 11:00a.m. Room 309 Panel - DBMS II: New Initiatives in Data Base Management Systems C. McBride, Chair, NSA Panelists: L. Vetter, Oracle; R. Varadarajan, Informix; M. Tinto, NSA; Dr. D Downs, The Aerospace Corporation

Room 307-308 **Issues in Trust & Specification** M. Woodcock, Chair, U.S. Naval Academy "Issues in the Specification of Secure Composite Systems" J. Hemenway, Grumman Data Systems "A Note on Compartmented Mode: To B2 or Not B2?" Dr. T.M.P. Lee, Trusted Information Systems, Inc. Room 317 Panel - Addressing U.S. Government Security Requirements for OSI N. Nazario, Chair, NIST Panelists: T. Humphreys, XISEC Consultants, U.K.; T. Bartee, IDA; D. Walters, NIST Room 301-303 **Trusted Networks** R. Kenneth Bauer, Arca Systems, Inc. Room 319-321 Panel - ISSA Initiatives D. Gary, Chair, Carnegie Mellon University 2:00p.m. Room 309 Panel: The Electronic Certification: The Time has Come, Part I M. Smid, Chair, NIST Panelists: C. Martin, Government Accounting Office; B. Johnson, Army Corp of Engineers; K. Rose, NSA; Room 307-308 "The New TPEP Process" S. Nardone, Chair, NSA "Concept Paper - An Overview of the Proposed Trust Technology Assessment Program", P. Toth, NIST Room 317 Panel: Forming A Computer Security Incident Response Capability (CSIRC) D. Steinauer, Chair, NIST Panelists: R. Pethia, Carnegie Mellon University; Dr. E. Schultz, Eugene Schultz and Associates; J. Wack, NIST Room 301-303 **Trusted Database Systems** Dr. G. Smith, Arca Systems, Inc. Room 319-321 Panel: Publications, Services, and Bulletin Boards R. Lau, Chair, NSA Panelists:

C. Hash, NSA; S. Radack, NIST; M. Schanken, NSA; M. Swanson, NIST

Room 305 2:00p.m. - 5:30 p.m. Group Decision Support for Developing a Curriculum DACUM Dr. Corey Schou, Idaho State University 4:00p.m. Room 309 Panel: The Electronic Certification: The Time has Come, Part II D. Dodson, Chair, NIST Panelists: G. Ostrem, Datakey; W. Bialick, NSA; L. Shomo, NASA; L. McNulty, NIST Room 307-308 Panel and Paper Current Information Security Initiatives within the U.S. Armed Forces LTC R. Ross, Chair, USA "Standard Certification - Progression" Captain C. Pierce, USAF, AFCSC Panel Discussion: Challenges Facing Certification and Accreditation Efforts of the Military Services Panelists: B. Zomback, U.S. Army; L. Merritt, U.S. Air Force; J. Mildner, U.S. Navy Room 317 Panel: Health Care G. Lang, Chair, The Harrison Avenue Corp. "Application Layer Security Requirements of a Medical Information System" D. Hamilton, Hewlett Packard Panelists: B. Bahramian, Beta Management Systems, Inc.; P. Fallon, Toshiba America Information Systems; S. Price-Francis, Canon Canada, Inc.; M. Schwartz, Summit Medical Systems, Inc. Room 301-303 **Trusted Integration & System Certification** J. Sachs, Arca Systems, Inc. Room 319-321 Student Papers Dr. H. Highland, Chair, Compulit "PM: A Unified Automated Deduction Tool for Verification" G. Fink, UC Davis

"Finding Security Flaws in Concurrent and Sequential Designs Using Planning Techniques" D. Frincke, UC Davis

"Electronic Measurement of Software Sharing for Computer Virus Epidemiology" L. de La Beaujardiere, UC Santa Barbara

October 15 9:00a.m.

Room 309 Panel - Intrusion Detection: Can we Build Models of Intrusions T. Lunt, Chair, SRI International Panelists: T. Garvey, SRI International; S. Snapp, Haystack Laboratories, Inc.; D. Icove, FBI; Dr. K. Levitt, UC Davis Room 307-308 Certification & Accreditation Experiences in Civil Agencies A. Friedman, Chair, The MITRE Corporation "Accreditation: Is It a Security Requirement or a Good Management Practice?" T. Anderson, USATREX International Inc. Panelists: S. Smith, FAA; P. Camero, DEA; F. Brant, DoS; W. Donovan, FEMA Room 317 **Operational Policies** R. Shilinski, Chair, NCSC "Some More Thoughts on the Buzzword "Security Policy"" D. Chizmadia, NSA "Operational Support of Downgrading in a Multi-Level Secure System" D. Nelson, Digital Equipment Corporation "Security Within the DODIIS Reference Model" B. McKenney, The MITRE Corporation Room 301-303 **Trusted Systems Concepts** Dr. C. Abzug, National Defense University Room 319-321 Panel: The National Research Educational Network (NREN): A Proposed Security Policy & Status Report S. Wolff, Chair, National Science Foundation Panelists: Dr. D. Branstad, NIST; Dr. S. Kent, BBN; Dr. S. Crocker, Trusted Information Systems, Inc.; V. Cerf, CNRI Cryptography Dr. H. Highland, Chair, Compulit "New Dimensions In Data Security" K. Mundt, CE Infosys "The Kinetic Protection Device" M. Bianco, Hughes Aircraft Company "Provably Weak Cryptographic Systems" Dr. J. Higgins, Brigham Young University 9:00-11:00a.m. Forming an Incident Response Capability Dr. Gene Schultz, Eugene Schultz and Associates 11:00a.m. Room 309

Panel: Security Protocols for Open Systems

P. Lambert, Chair Motorola Panelists: R. Housley, XEROX; D. Maughan, NSA; D. Solo, BBN; D. Walters, NIST; M. White, Booz-Allen & Hamilton Room 307-308 **INFOSEC** Design and Certification Initiatives D. Arnold, Chair, NSA "General Issues to be Resolved in Achieving Multilevel Security " W. Neugent, The Mitre Corporation Panelists: CDR. D. Campbell, USN, NSA; R. Flowers, NSA; S. Westendorf, NSA Room 317 Panel - What Senior Federal Managers Think About Security C. Bythewood, Chair, NCSC E. Springer, Office of Management and Budget I. Gilbert Perry, NIST

Room 301-303 Trusted Networks J. Sachs, Arca Systems Inc.

Room 319-321 Panel: Federal Information Systems Security Educators' Association (FISSEA) Dr. W. Maconachy, Chair, NSA Dr. C. Schou, Idaho State University; J. Pohly, U.S.A.F.; D. de Zafra, Public Health Service; V. Marshall, Booz-Allen & Hamilton;, B. Guffie, Social Security Administration

Room 323 Intrusion Detection T. Lunt, Chair, SRI International "Intrusion and Anomaly Detection: ISOA Update" J. Winkler, PRC, Inc.

"Internetwork Security Monitor: An Intrusion Detection System for Large Scale Networks" T. Heberlein, University of California - Davis

2:00p.m. Room 309 ACCESS CONTROL D. Dodson, Chair, NIST "Role Based Access Control" R. Kuhn, NIST "Knowledge-Based Inference Control in a Multilevel Secure Database Management System" Dr. B. Thuraisingham, The MITRE Corporation "A TCB Subset For Integrity and Role-Based Access Control" D. Sterne, Trusted Information Systems, Inc.

Room 307-308 Multilevel Security (MLS) Prototyping and Integration: Lessons Learned and DoD Directions C. West, Chair, Defense Information Systems Agency Panelists: R. Hale, NRL; Major R. LeSieur, USAF, ESC; E. Schwartz, NSA; C. Cross-Davison, DIA Room 317 PANEL - Privacy I - Domestic Privacy: Roll of Honor and Hall of Shame W. Madsen, Chair "E-Mail Privacy and the Law" C. Axsmith, Esq., ManTech Strategic Associates, Ltd. Panelists: L. Schaefer, The MITRE Corporation; J. Abernathy, The Houston Chronicle Room 301-303

Trusted Database Systems Dr. G. Smith, ARCA Systems, Inc.

Room 319-321 Considerations for Assurance T. Malarkey, Chair, NSA "A Model of Risk Management in the Development Life Cycle" Capt C. Pierce, USAF, AFCSC "Concept for a Smart Card Kerberos" M. Krajewski, Jr., The MITRE Corporation "Operating System Support for Trusted Applications" R. Graubart, The MITRE Corporation

"Potential Benefits from Implementing the Clark-Wilson Integrity Model Using an Object-Oriented Approach" C. Schiller, Science Applications International Corporation

Room 323 Defense Against Computer Aids H. Peele, Air Force Intelligence Command

Room 305 2:00-5:30 p.m. Making it Work: Applying INFOSEC to the Real World C. Barker, T. Parenty-Winkler, Trusted Information Systems, Inc.

4:00p.m. Room 309 Data Assurances Profesor S. Jajodia, Chair, George Mason University

"Integrity and Assurance of Service Protection in a Large, Multipurpose, Critical System" H. Johnson, Information Intelligence Sciences, Inc.

"An Example Complex Application for High Assurance Systems" S. Padilla, SPARTA

"Mandatory Policy Issues of High Assurance Composite Systems" J. Fellows, Grumman Data Systems

Room 307-308 Trusted Network Products P. Woodie, Chair, NSA "Towards a Policy-Free Protocol Supporting a Secure X Window System" M. Smith, AT&T Bell Laboratories "An SDNS Platform for Trusted Products" E. Borgoyne, Motorola "SDNS Security Management" W. Jansen, NIST

Room 317
Panel: Privacy II - International Data Privacy: Roll of Honor and Hall of Shame
W. Madsen, Chair, CSC
Panelists:
G. Montigny, Privacy Commission of Canada; E. Hendricks, Privacy Times

Room 301-303 Trusted Integration & System Integration Dr. W. Wilson, Arca Systems Inc.

Room 319-321 Trust Documentation W. Geer, Chair, AFCSC "Current Endorsed Tools List (ETL) Examples: Lessons Learned" C. Garvey, TRW Systems Integration Group

"Companion Document Series to the Trusted Database Management System Interpretation" L. Notargiacomo, The MITRE Corporation

"Assessing Modularity in Trusted Computing Bases" Dr. D. Baker, The Aerospace Corporation

Room 323 Panel: Electronic Crime: An Investigative Perspective Jack Holleran, Chair, National Computer Security Center Speakers: Special Agent Jack Lewis, Electronic Crimes Branch, Secret Service Special Agent Mark Pollett, Federal Bureau of Investigation

October 16 9:00a.m. Room 309 Panel: R&D Future Needs B. Snow, Chair, NSA Panelists: Dr. S. Kent, BBN; W. Boebert, Secure Computing Corporation

Room 307-308 Information Security Engineering ENS S. Mitchell, USN, Chair, NSA

"Information System Security Engineering: Cornerstone to the Future" Dr. D. Howe, NSA

"Network Security via DNSIX, Integration of DNSIX and CMW Technology"

H. Heller, Harris Corporation
"Issues to Consider When Using Evaluated Products to Implement Secure Mission Systems" Lt Col W. Price, USAF, Air Force Space Command
Room 317
Panel: Privacy III -Government Surveillance Policy and Capabilities as the Telephone Network Goes Digital --- The FBI's Digital Telephony Initiative Dr. L. Hoffman, Chair, George Washington University
Panelists:

A. Bayse, FBI; J. Edwards, NORTEL Federal Systems, Inc.;
J. Podesta, Podesta Associates

Access Policies Mechanisms M. Schaefer, Chair, CTA, Inc.

"Implementation Considerations for the Typed Access Matrix Model in a Distributed Environment" G. Suri, George Mason University

"A Lattice Interpretation of the Chinese Wall Policy" Professor R. Sandhu, George Mason University

"Experience with a Penetration Analysis Method and Tool" Dr. S. Gupta, University of Maryland

Room 319-321 Data Distribution K. Rowe, Chair, NSA

"A Tamper-Resistant Seal for Trusted Distribution and Life-Cycle Integrity Assurance" M. Bianco, Hughes Aircraft Company

"Use of a Case Tool to Define the Specifications of a Trusted Guard" R. Lazar, The MITRE Corporation

"A Security Reference Model for a Distributed Object System and its Application" V. Varadharajan, Hewlett-Packard Labs., U.K.

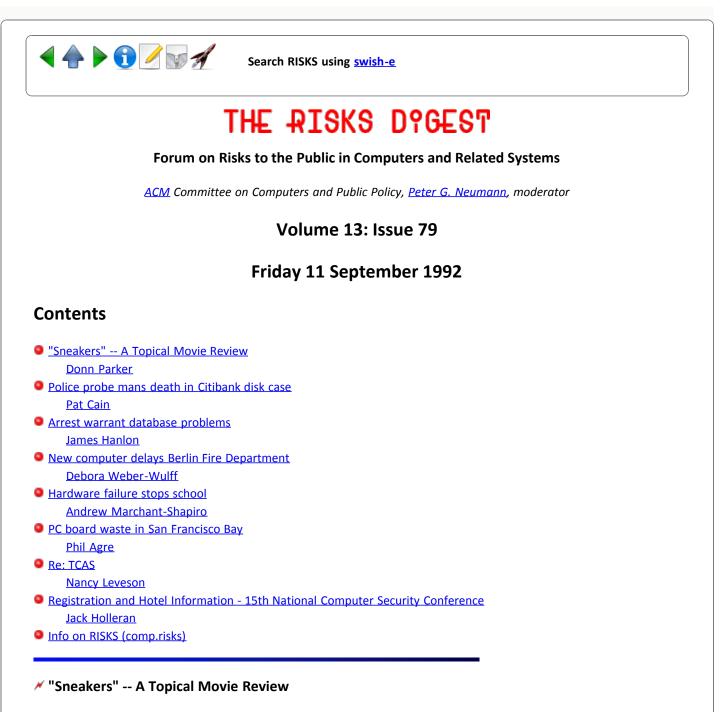
Room 305 9:00a.m. - 5:30p.m. Intrusion Detection Workshop Teresa Lunt, SRI International



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 13: Issue 78



## <donn\_parker@qm.sri.com> 11 Sep 1992 08:00:03 -0800

[The following review was prepared by Donn Parker for distribution to the members of the International Information Integrity Institute (known as I-4), an organization consisting of something like 60 companies with significant interest in improved computer security and integrity, which is managed by SRI -- with Donn as one of its key players. This review is reproduced here with his permission, and is authorized for further distribution, with appropriate attribution. Sneakers opens today to the general public, although in a few selected theaters it opened on Wednesday, presumably to get early reviews. (Both Donn and I had been visited by Parkes and Lasker regarding security risks, in their preparation for the screenplay for WarGames. They even used some of our ideas. In general,

Sneakers seems technologically sounder, and is certainly of interest to RISKS readers. For those of you who don't know Donn, he is often referred to as the Great Bald Eagle of Computer Security.) PGN]

FILM REVIEW OF SNEAKERS by Donn B. Parker September 1992

Sneakers (released September 11, 1992 by Universal Studios, owned by Matsushita Electric Industrial Co. Ltd., and promoted in association with CompuServe, owned by H&R Block) starring Robert Redford, Dan Aykroyd, Ben Kingsley, Mary McDonnell, River Phoenix, Sidney Poitier, and David Strathairn; directed by Phil Alden Robinson (Field of Dreams director); and produced and written by Walter F. Parkes and Lawrence Lasker (writers and producers of WarGames in 1981).

The new computer crime movie, Sneakers (as in hackers who wear sneakers and sneak into computers) was previewed in a San Francisco showing sponsored by Universal Studios and Mondo 2000 Magazine (a slick-cover psychedelic publication of the Timothy Leary genre appealing to hackers) and attended by a large segment of the Bay Area hacker community including Cap'n Crunch. I had assisted the writers, Messrs. Lasker and Parkes, with their first movie, Wargames-much to my chagrin because the technology was so distorted. This time they had the technical assistance of Len Adleman (the A in RSA Crypto) from USC and Robert Abbott, an information security consultant of long standing. This Mission Impossible, PG-rated (only three "God damn"s and almost no sex) film is mostly technologically believable, unlike Wargames. We can forgive them for showing a Cray computer with a terminal displaying Windows 3.1.

All information security professionals should see this film and use it to promote security awareness. Some critics may pan it, but it has all the ingredients for financial success. It has:

- o great chase and other street action scenes in the beautiful San Francisco Bay Area
- o an interesting but predictable plot
- o the blind technician who finds the bad guys' hideout from sounds heard from the trunk of a car
- the old technique of the bad guy shooting into the ceiling tiles at his hidden enemy hiding in ceiling duct area
- o three bloodless murders
- o total unconsciousness produced by simple taps on the head followed by immediate concussion-less revival with little visible damage
- o popular stars, Redford, Poitier, Aykroyd, and Kingsley, who look like the oldest hackers in the world (except for me and Cap'n Crunch)
- great human melodrama with good character development and not too much technical sci-fi stuff
- o the good guy and his girlfriend at the mercy of the bad guy in the grand finale
- o cryptography very well explained and used for a general audience
- o the proverbial spinning computer tape drive, and

o as usual with Lasker and Parkes, a moral at the end.

Universal has uniquely teamed up with CompuServe and CompUSA computer stores to promote the movie. A chat board has been set up to fire questions about the movie at Mr. Robinson, the director, who has been using CompuServe for 8 years. Anagram and secret password games can be played, with prizes including trips to Hollywood and Robert Redford's jacket worn in the film. The film is sure to be a big hit in Europe and Japan as well as in the United States and should appeal to the juvenile hacker culture throughout the world.

One unbelievable item is the skimpy \$175,000 accepted by Redford's security penetration (read "tiger team") consulting company for a record-breaking information security project. Redford's team plus all the high-priced technical equipment were worth much more than that. They had to steal the universal decryption black box-the Maltese Falcon of the movie-and then steal it again from the bad guys posing as NSA types who steal it from Redford. There is a neat shoulder-surfing password pickup by video recording. There are hacker antics such as a transfer of President Nixon's net worth to the National Organization for the Reform of Marijuana Laws (NORML), credit record and license plate registration privacy invasions, trashing of the NSA, CIA, and FBI, and liberal-politics slams at President Bush and the Republican Party well-timed for the upcoming national elections. However, this is all tolerable since it is done by Redford's character and his team who all have serious criminal and other highly unethical practices in their backgrounds.

A tiger team attack on a client bank that has relatively good security is excessively elaborate and would have left the bank guard in a good position to sue his employer for aggravated assault and mental anguish. We will probably have to assure our company management people that we don't do things like that-but the time to justify your budget and staff is soon after they see this movie.

The film ends with the rather patronizing and simplistic advice that whoever controls the information, controls the world. Just the straightforward action and technology without all the liberal politics and moralizing would have made it even better.

You and your teenage children and your computer users and management should all see and enjoy this much-to-be-talked-about film.

### Police probe mans death in Citibank disk case

Pat Cain <cain\_p@kosmos.wcc.govt.nz> Wed, 09 Sep 1992 13:24:18 +1200

Early on Saturday (5th Sept) morning in Auckland, New Zealand, Paul Gordon Edward White, 26, a computer broker, was found in a crashed car by the Auckland harbour bridge; he died shortly afterwards. A police investigation into the accident began. But last night (Tuesday) the Police Minister, John Banks, asked police to begin high priority investigations into allegations that his death may not have been accidental. White had purchased \$525 of surplus office and computer equipment from Citibank in Auckland. Accidentally included with the equipment were around 90 computer disks. TV3 reported the disks contained details overseas bank accounts of some politicians and of some companies laundering money overseas. White is understood to have offered to sell the material back to the bank for \$50,000. In an out-of-court settlement on Friday, Citibank paid White \$15,000 cash for the return of all outstanding information in his control. The suitcase in which White had the money was found in the car along with his body, but the money was missing.

White's lawyer, Mark Blomkamp told TV3 that someone may well have considered the information on the disks serious enough to kill for. Asked if it was possible that because the money was not in White's briefcase in his crashed car the accident could have been invoked, Blomkamp said: "You might well think that but I couldn't possibly comment".

Radio NZ last night quoted an unidentified source saying that White's car was not as badly damaged as could be expected from an impact with a concrete pillar. The front of the car was significantly damaged by the 5.15am crash on the Fanshawe St, city side, approach to the harbour bridge, but the dashboard and steering wheel were not and there was no blood in the vehicle.

Bits and pieces ..

- \* Neighbours reported White's home in Birkenhead had been broken into several times and that he had met Tauranga MP Winston Peters (who is a member of the current government and several months ago alleged government links with big business and corruption).
- \* In one of three earlier burglaries, White was attacked as he returned home one night.
- \* White reported that in July he had been approached by people who identified themselves as members of the Security Intelligence Service, wanting to discuss the Citibank information. After the meeting, White told an acquaintance that the supposed SIS agents had warned him that the police were about to search his property. The search took place two days later. (NZSIS is NZ's approximate equivalent to the US's CIA.)
- \* On Friday, White celebrated at the Centra hotel in Auckland, he then left with a man and a woman (who have since been interviewed) at 10pm and went to the Regent Hotel for a meal. After that he went to a nightclub and left about 4am. What happened between then and 5.15am when he was found is unclear.
- \* Citibank is the New Zealand subsidiary of one of the largest banks in the United States, Citicorp. It operates as a clearing bank and provides a range of non-retail banking services.
- \* The Ambulance service received "two or three" emergency calls from mobile phones -- it is not known who made the calls, or whether they witnessed the car crash. White died shortly after the ambulance arrived.

(Summarized from {The Dominion} and {The New Zealand Herald}, 9 Sept 1992).

### Arrest warrant database problems

James Hanlon <tcubed@ddsw1.mcs.com> Wed, 9 Sep 92 17:01:51 CDT

Note: I recently posted a similar note to misc.legal.computing; I suspect the problem is common enough to enlist the help of the RISKS community.

An attorney acquaintance has a number of clients who have been picked up and detained for various lengths of time, on the basis of warrants, later shown to be incorrect. Reasons range from sloppy administrative work (clerical errors, name confusions), to accumulated delays in the record-keeping process.

#### BACKGROUND INFORMATION

Police officers in the US need a few things in order to take a person into custody ("arrest" them): chief among them is probable cause to believe that they have committed a crime. The fact that an arrest warrant exists is in itself probable cause. In practice, one can be taken into custody if the arresting officer believes that a warrant exists--and someone on the radio telling him that "the computer" shows an outstanding warrant is reason enough.

Problems occur in areas where numerous law enforcement agencies overlap, i.e., most urban areas in the US. Although there is normally a regional database of warrant information, any agency can keep a database of warrants its own officers have issued. Should a judge order a warrant killed ("quashed" is the legalism), and should the kill order not be properly accomplished, the stage is set: person leaves courtroom relieved, goes about his business, is stopped some months (or years) later, officer checks central database, finds warrant information, calls warrant-issuing police department, which checks \*\*its\*\* warrant database. Conclusion: you are under arrest. There follows a collection of more or less unpleasant and inconvenient experiences (e.g., a weekend in the county lockup).

My question: is there an archive of these, or similar, occurrences on the net? Is there a model of how the problem should be solved, perhaps in Jurisdiction X?

I should mention that the attorney is presently suing the government units involved, in federal district court in Chicago.

Thanks for all help.

James E. Hanlon

tcubed@ddsw1.mcs.com

### New computer delays Berlin Fire Department

Debora Weber-Wulff <weberwu@inf.fu-berlin.de> Tue, 8 Sep 1992 10:11:09 GMT

Sigh. It's like no one reads comp.risks :-(.

The "Tagespiegel" announced this morning that the Berlin Fire Department has been having terrible trouble with it's new dispatching system. Seems they went

on line after just a few "tests" (no running the system in parallel to the old one) because they now have to take care of the whole city and not just West Berlin. They are having problems with fire-trucks being listed more than once, phantom fire trucks, disappearing fire-trucks and messages, and the wrong trucks being alerted. Seems the data entry people or the algorithm for finding the closest fire station (or both) are not working, and trucks are being called from far away, or they are alerted and then not told where to go. There have been cases of it taking 30 minutes to get a fire truck to the scene of a fire.

Not a nice thought when youths are increasingly setting fires to refugee hostels and such.

The company that installed the program is busy fixing the bugs, the newspaper assures us, and will have it running soon. Won't we all sleep better knowing that it is sure to run when that last bug is gone?!

Debora Weber-Wulff, Institut fuer Informatik, Nestorstr. 8-9, D-W-1000 Berlin 31 +49 30 89691 124 dww@inf.fu-berlin.de

### Mardware failure stops school

"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu> 9 Sep 92 15:16:00 EST

My institution, Union College, fell victim to a computer problem today: A Hewlett-Packard machine used to handle registration died, leaving the College unable to complete freshfolk registration. Consequently, classes that were scheduled to start on 9/10 cannot meet until next Tuesday, and an extra day (or two??) will have to be added to the term calendar to make things work out. All faculty received notices marked URGENT that spoke of a 'massive computer failure.'

I have little data on the failure, other than that it was apparently NOT a software failure, but a real hardware breakdown.

Now, I suppose that the software and data on that machine are backed up -- but there's the rub. What do you do when you only have one piece of HARDWARE? It's ironic, because most of the campus is hooked up to a 3-machine VAX cluster -- while Administration runs on the single HP. Good for security, but bad for reliability. Since many of the copiers went down at the same time (yep, in the midst of syllabusing) I suspect a technological conspiracy...;-)

Andrew Marchant-Shapiro, Depts of Sociology and Political Science, Union College, Schenectady NY 12308 (518) 370-6225 marchana@union.bitnet

## PC board waste in San Francisco Bay

Phil Agre <pagre@weber.ucsd.edu> Wed, 9 Sep 92 17:11:53 -0700

The lead article in the current issue of "Global Electronics" (issue 115,

August 1992) concerns the pollution of San Francisco Bay by heavy metals running off from small printed circuit board assembly shops in Silicon Valley. It traces the problem to the common electronics industry practice of subcontracting to these small firms rather than doing the dirty work in larger and safer facilities of its own. "Global Electronics" is published by the Pacific Studies Center, 222B View Street, Mountain View CA 94041. It costs \$12 per year (12 issues of four pages each).

Phil Agre, UCSD

## Re: TCAS (<u>RISKS-13.78</u>)

Nancy Leveson <nancy@murphy.ICS.UCI.EDU> Fri, 04 Sep 92 16:23:40 -0700

#### >From **RISKS 13.78**,

In the version of the TCAS story I saw locally about the 2 USair jets near-miss, it mentioned that for the period june -June of the previous year, over 60% of the warnings/advisements from TCAS systems nationwide have been erroneous. Many of these have been of the same sort reported -- the system told two planes that were "safe" to maneuver into an "unsafe" flight path...

This is totally and completely untrue and is evidence of what I warned about in my previous message. Even if you don't have the facts, does anyone seriously think that a system with this error rate would be used at all? Pilots are just not that stupid or suicidal and neither are those at the FAA..

It is very important that forums such as RISKS do not become sources of dangerous misinformation.

[I agree. I have been somewhat too lenient in recent times, permitting material to emerge that is lacking in credibility, scholarship, carefulness, etc. Time to ratchet up the quality again. But I am very much at the mercy of our contributors. Please observe the masthead guidelines. Thanks. PGN]

#### Kegistration and Hotel Information - 15th National Computer

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL> Wed, 9 Sep 92 11:10 EDT

Security Conference

The following information includes registration and hotel information for the upcoming 15th National Computer Security Conference. Appropriate phone numbers are included. (The program is contained in <u>RISKS-13.78</u>.)

=-+-=

CONFERENCE REGISTRATION FORM 15th National Computer Security Conference

Baltimore, Maryland	
NAME:	
COMPANY:	
ADDRESS:	
CITY:	STATE: ZIP:
COUNTRY:	TELEPHONE NO:
HOW WOULD YOU	LIKE YOUR NAME TO APPEAR ON YOUR BADGE?
-	30.00 before October 1, 1992; In or after October 1, 1992
Payment Enclosed ir Form of Payment:	n the Amount of:
Compute	e checks payable to NIST/15th National r Security Conference. All checks drawn on U.S. banks only.
Purchase Or	der Attached. P.O. No.:
Federal Gove	ernment Training Form
	Visa Exp. Date
Authorized Sig	gnature:
PLEASE NOTE: No o	ther credit cards will be accepted.
Please return confer	rence registration form and payment to:
Office of the C National Instit	ute of Standards and Technology Idministration Building
Credit card reg	gistration may be faxed to
Tammie Grice	e at (301) 926-1630.
	you have attended the National Computer Security

<ul> <li>I do want my name on the Conference Participants List which is distributed to conference attendees.</li> <li>I do not want my name on the Conference Participants List.</li> </ul>
=-+-=-+-=-+-=-+-=-+-=-+-=-+-=-+-=-+-=-+
HOTEL RESERVATION FORM 15th National Computer Security Conference October 13-16, 1992 Baltimore Convention Center Baltimore, Maryland
Hyatt Regency Baltimore(410) 528-1234300 Light StreetBaltimore, MD 21202
Holiday Inn Baltimore Inner Harbor (410) 685-3500 301 West Lombard Street Baltimore, MD 21201
Radisson Plaza Baltimore Hotel (410) 539-8400 20 West Baltimore Street Baltimore, MD 21201
Tremont Plaza (410) 727-2222 222 St. Paul Place Baltimore, MD 21202 (An all suites hotel)
Baltimore Marriott Inner Harbor (410) 962-0202 110 South Eutaw Street Baltimore, MD 21201
Tremont Hotels(410) 576-12008 East Plesant StreetBaltimore, MD 21202(An all suites hotel)
NAME: COMPANY: ADDRESS:
CITY: STATE: ZIP:
COUNTRY: TELEPHONE NO: (include country access code if appropriate)
Please Reserve: Single Room(s) Double Room(s)
Arrival Date: Departure Date:
Person Sharing Room:

RATE (Refer to Conference Brochure):Corporate;Government
Method of Guarantee:Deposit Enclosed; Credit Card
Check One: American Express VisaMasterCardDiners ClubCarte Blanche
Credit Card #: Exp. Date:
Signature of Cardholder:
✓ ♠ ▶ ① ☑ ✓ Search RISKS using swish-e
Report problems with the web pages to <u>the maintainer</u>



# Arrest Warrants

Joseph Nathan Hall <joseph@joebloe.maple-shade.nj.us> Sat, 12 Sep 92 13:57:25 EDT

The son of a former employer of mine was met at the door one Saturday morning by two local police officers, who presented him with a felony arrest warrant and took him off to jail. The charges involved were something like passing bad commercial paper and perhaps interstate flight. I gather that he was a little surprised.

It turned out that he had left some money in a checking account in a bank in another state (Missouri, I think) before moving to his new residence. After a

while, the service charges ate up the funds in the account and the last charge "bounced." The bank treated it as a bad check. They looked for him for a while, and then, since bad paper in the state in question is a felony, regardless of the amount, they passed the info to the local authorities and an arrest warrant resulted. (I wonder whether there was any human intervention up to the point where the judge issued the warrant.)

Apparently there is a pretty good interstate commerce in arrest warrants, and somehow the out-of-state warrant wound up at the local police station, along with the "suspect's" current address. Most stations keep a pile of warrants that need to be served handy for slow times--like Saturday morning.

#### It could happen to YOU!

Disclaimer: This story was related to me a few years ago by a former employer. I believe that the facts as I have stated them are essentially correct, though the details are no longer clear in my memory.

uunet!joebloe!joseph (609) 273-8200 day joseph%joebloe@uunet.uu.net 2102 Ryan's Run East, Rt. 38 & 41, Maple Shade NJ 08052

### Stop the presses, call the police!

<Frans.Heeman@cwi.nl> Tue, 15 Sep 1992 07:53:35 GMT

[From the Dutch national paper "De Volkskrant", September 3, 1992:]

On Saturday morning, August 29, the presses at the local newspaper "De Gelderlander" went down, causing delivery to be delayed. Many subscribers called the newspaper at its phone number 650611. The telephone exchange at the newspaper got jammed. One of the consequences was, that when people tried to call the newspaper, often only the last four digits, 0611, came through. Now it happens that 0611 is the national emergency number in the Netherlands. So the police was swamped with calls from people, informing about the delivery of their newspaper, jamming the emergency number. In a reaction, the PTT said that they would be careful with giving numbers ending in 0611 to large companies.

Frans Heeman, CWI dept. of Interactive Systems, Kruislaan 413, 1098 SJ Amsterdam P.O. Box 4079, 1009 AB Amsterdam frans@cwi.nl phone: +31 20 592 4164

### A Financial risk avoided

# <HORN%athena@leia.polaroid.com> Fri, 11 Sep 1992 14:29 EST

In light of all the financial problems that get reported I decided to recognize a firm that made an intelligent decision. Recently Citizen's Utilities had a stock split: 3 for 2. People who use the dividend reinvestment alternative generally have fractional share balances. So someone with 0.70 fractional shares would now have 1.05 shares. Rather than merge the full shares from the split with the full share from the fractional share account, they chose to wait until the next regular quarterly dividend. At this time the routine processing shifts full shares.

In the letter accompanying the newly issued shares they called attention to this and gave the name of the person who could manually issue the extra share if for some reason you needed that share before the next dividend (about ten weeks later). They gave the reason for all this as:

excessive programming complexity

Considering how few people will need that one share certificate during the next ten weeks I think they made a good choice by sticking to the regularly used and reliable procedures, providing a manual override, and informing their owners.

We usually hear about various kinds of mistakes, oversights, and maliciousness. It is also appropriate to point out things done well.

Rob Horn horn%hydra@polaroid.com

### From the Jury Room - Alcohol breath analyzer

Jim Haynes <haynes@cats.UCSC.EDU> Sun, 13 Sep 92 22:00:43 -0700

I was on a jury last week (trial now over so I can talk about it) and part of the case involved a breath alcohol machine. We were not shown the machine but it was described by expert witnesses and we saw its output. The machine in question is microprocessor controlled and displays two digits of output - any other significance is truncated. To use it the officer first puts a blank card into a slot and types in the suspect's name and date and time and the like. The machine prints all this on the card along with the test results. The test consists of an air purge, when the machine checks itself for a zero reading; then the suspect blows; then another air purge and zero check; then another blow; then a final air purge and zero check and all these results are printed on the card. During the blowing a tone sounds to signal that the suspect is blowing hard enough.

Whatever it is the machine measures, it takes a measurement every 0.6 seconds and waits for three of these to be the same before treating that as a reading. Hence as the alcohol concentration in the blow increases the machine is supposed to wait for a plateau and record the plateau value. The machine is supposed to measure and subtract something else to eliminate the effects of substances such as acetone that were known to throw off earlier model machines.

Supposedly the calibration of the machine is fixed at manufacture; but the calibration is verified about once a week by the forensic lab which takes care of it. There is an alcohol-water solution in a breath simulator attached to the machine. The lab dials up using a modem and commands the machine to verify its calibration. The machine measures the simulated breath and sends the measurement and its identification back to the lab, where the information is kept in their computer and can produce a printed report as needed. The test

solution is supposed to make the machine read 0.14% +/- 0.01%.

For the machine in question there was a verification a few days before the crucial test, and another one a few days later. Both times the machine read 0.15%, which is acceptable. We saw the results of several other verifications and this machine usually read 0.15%, although once or twice in the past it had read 0.13%. On the test in question the machine had read 0.09% . A blood alcohol level of 0.08% makes it illegal to drive a car in California.

I convinced myself and the rest of the jury that a blood alcohol level of 0.08% in the defendant was unproven. First, when the machine read 0.15% that could mean anything between 0.1500... and 0.1599... Second, we were not told any more about the test solution than that it should produce a reading of 0.14%. I know chemists can mix up solutions very accurately, and for good science you would want to mix the solution as close to 0.14500... as possible; but we had to assume the solution could be anywhere between 0.1400... and 0.1499... So we could have a solution at the high end of 0.14 and the machine could be measuring at the low end of 0.15 and it is measuring pretty close. Or we could have a solution at the low end of 0.14 and the machine could be measuring at the high end of 0.15 and it is off by just under 0.02%. If errors are additive offsets then the defendant's blood alcohol could be anywhere between 0.0700... and 0.0899... and that absolutely fails to prove 0.08% or more. I used an analogy at the time that this is like trying to verify the accuracy of a yardstick by comparing it with another yardstick.

There's an interesting psychological phenomenon that I observed. There was a lot of testimony by experts about errors and possible errors in the machine. Invariably they and the attorneys would add and subtract 0.01 here and 0.02 there from machine readings as if all the errors are additive offsets. There was never any testimony as to whether the errors in the machine are really offsets or proportional to the reading, or completely nonlinear, or anything else. Nobody ever mentioned an error of so many per-cent, or suggested that multiplication be used. So I conjecture: when people deal with numerical data where there are only two digits they tend to assume that any adjustments to the data are to be made by addition and subtraction. Maybe this phenomenon results from habit dealing with dollars and cents; or maybe it's just that people are lazy and addition is easier than multiplication.

Both experts agreed that the readings are affected by the suspect's body temperature. I was surprised that the machine doesn't measure and correct for this, or that the temperature isn't taken and recorded at the time of the test.

If we had not been doubtful of guilt from the above accuracy considerations alone we would have had to consider the defense expert's suggestion of various confounding factors, a much more speculative undertaking. He and his colleagues have done experiments and published in the field. They have a few instances in which the subject got a false high reading by blowing very hard. This is not fully understood. He said something about the mucous membranes drying out and releasing extra alcohol. He drew a graph showing that the machine sees a first plateau, at which the reading is good; but then the alcohol level increases and goes to a second higher plateau and the machine takes that as its reading instead of the first. They have also found the machine will read too high if the suspect is still absorbing ingested alcohol, which can happen for example if the alcohol was taken with food. He didn't offer an explanation for this, but only evidence that it can happen.

There are formulas to predict blood alcohol level based on the amount of alcohol ingested and the weight of the subject and other factors. Our defendant admitted to drinking only one pint of stout with food about 2 hours before the arrest. Both experts calculated this was not enough alcohol to get anywhere near 0.08% blood alcohol. It was maybe barely enough to get the machine to read 0.09% with all of the confounding factors such as temperature and blowing hard and the absorptive-phase phenomenon. Maybe she drank more than she admitted; maybe the machine really is that lousy inaccurate; maybe there are other unconsidered factors leading to errors; we didn't have to go into that.

Advice to drivers would seem to be: if you are arrested for DUI and believe you are innocent then don't choose the breath test - it's not very accurate. If you think you might barely be guilty then choose the breath test and fight it in court.

## Automatic DUI (Driving Under the Influence)

Jane Beckman <jane@stratus.swdc.stratus.com> Mon, 14 Sep 92 17:50:55 PDT

A friend's husband just recently got a shock. A notice showed up in the mail that his driver's license was suspended. He called up the California Department of Motor Vehicles (DMV) to find out what was going on. He had recently been involved in a dispute involving his auto, so he suspected it might have something to do with that.

Well, they asked him, didn't you recently plead guilty to a charge of Reckless Driving? Yes, he said. Well, that explains it. Wait a minute, he said, explains what? He said it was his understanding that Reckless Driving was not something they normally pulled your license for, or he would have fought it. Oh no, they said, that was for the liquor. You have a DUI (Driving Under the Influence). WHAT? he asked. Your Reckless Driving in connection with DUI. At this point, he knew he had a problem since there was no alcohol involved.

He explained to the woman that the Reckless Driving charge was a plea bargain. He had been stopped and threatened by a juvenile gang who had blocked his car. He had stepped on the gas and hit one of them in trying to get out of there. He was charged with Battery and Assault With a Deadly Weapon (his car) by the gang member, who pressed charges. His lawyer had advised him that fighting the charge, despite circumstances, would be a long and costly battle, especially since where juveniles were involved, it was possible that the jury would find against him. They plea-bargained to a lesser charge of Reckless Driving, and he was fined \$250 and sentenced to do 60 hours of community service work (which he was doing, anyway).

Fine up until that point. The woman at the DMV insisted that there was a DUI on the record. He explained all of the above, and she asked where the liquor came into it. He explained that there was \*never\* any liquor involved. Finally, he went down to the office and hassled with the officials there, and

the court records were pulled. Surprise, no DUI! It was entered into the system again, and bingo, a DUI came up. I suspect that regular RISKS readers already suspect what the problem was. The system programming on traffic offenses was set up so that a count of Reckless Driving \*automatically\* entered in a paired count of Driving Under the Influence. The programmer had made the assumption that the two counts were so intimately connected that you would almost \*never\* have one without the other. To enter a count of Reckless Driving without a DUI, you had to manually override it, and the data-entry clerk was not instructed on this peculiarity, nor was there any flag that Reckless Driving was paired with DUI. And a "guilty" on that count was paired to an automatic license suspension. The problem of overriding the DUI was finally resolved, but it took several days and a lot of arguing hyperventilating on his part. I would suspect that his is not the first, nor the last, case where this "automatic conviction" came up.

Jane Beckman [jane@swdc.stratus.com]

### Ke: update: Barclay voice mail insecurity (Brunnstein, <u>RISKS-13.79</u>)

Flint Pellett <flint@gistdev.gist.com> 14 Sep 92 19:59:51 GMT

Northern Telecom requires for the US/Canada product \*at least 4
 >digits code\*, whereas the German version was reduced to require \*at least 3...

This discussion reminded me of something that I was involved in way back in 1979, which I think is still relevant. The point to be made is that merely the number of bytes in the codeword is insufficient protection. What matters is the product of the number of different combinations by the amount of time required to try each one. (I think this principle applies to other things such as garage door openers as well, and would love to see someone telling me that once my garage door opener circuitry has recognized that a code was sent which was not the right one, it would not respond to any other code (even the right one) for a period of, perhaps, 15 seconds.) I could then calculate that if there were 10,000 possible codes, that an automated attack would take an average of 20.5 hours, and know how lousy the protection was.) As it stands now, I don't really know how secure the system is, and I don't have any idea how secure the 4-digit or 3-digit codes above are.

The incident in question that I had experience with: note that I was not a part of the system staff, so parts of the following are 2nd hand information and may not be completely correct. This particular mainframe system allowed access to files based on the entry of a codeword, which could have up to 10 characters, and it was quite secure even if you used a 5 character password, given the fact that it would accept input at a maximum of 1200 baud: the average time required to enter all the codes even with a machine doing your typing was years. Normal users were not allowed to access files through programs. The obvious extension of allowing a user program to open a file was made, and the risk that a program could try passwords a lot faster than 1200 baud was noted. The solution adopted was to write the file opening code so that it would re-read the disk to get the password on every attempt: thus, the speed of the disk access limited the speed at which passwords could be tried, and given agonizingly slow disk performance, things were still secure. Unfortunately, at some time later disk cache software was incorporated into the system which made the system smart enough that it would not re-read something if it still had it available in memory. The result was that the 5 character passwords which had been pretty secure suddenly became worthless, because even a brute-force program to try all combinations would run in a few hours.

Bottom line: if you're trying to tell me how secure something is, don't tell me how many combinations there are on the lock, tell me how long it would take to try 1/2 of the combinations, and convince me that you have a way to insure that that time will not decrease as faster and more powerful hardware becomes available.

Flint Pellett, Global Information Systems Technology, Inc., 100 Trade Centre Drive, Suite 301, Champaign, IL 61820 (217) 352-1165 uunet!gistdev!flint

## Ke: "Sneakers" -- A Topical Movie Review (Parker, <u>RISKS-13.79</u>)

Mark Brader <msb@sq.com> Mon, 14 Sep 1992 02:06:00 -0400

Anyone who has not already seen "Sneakers", but would like to, should be careful to have NOT read <u>RISKS-13.79</u>, where a so-called review, right at the top of the issue, reveals most of the storyline and many of the nicer "touches", WITHOUT SO MUCH AS A SPOILER WARNING.

Mark Brader SoftQuad Inc., Toronto utzoo!sq!msb, msb@sq.com

[Donn Parker's review was written for his I-4 audience, consisting largely of corporate folks with serious security concerns. He was undoubtedly trying to encourage them to see the movie. Perhaps that review was less suitable for the RISKS audience, so I suppose next time Mark or I will have write a review specifically aimed at you all, tantalizing you without revealing any of the plot or technological devices. There are also lots of in-jokes, which will NOT appear here. Incidentally, Sneakers was ranked NUMBER 1 in box-office this week. PGN]

#### Re: Sneakers, the movie (<u>RISKS-13.79</u>)

Tri-Valley Macintosh Users Group,UG <TMUG@applelink.apple.com> 15 Sep 92 01:23 GMT

The phone number they mention in the movie "Sneakers" is a valid 510 area code number; it gets you the IRS in the East Bay. I wonder if this was a glitch. (Movies usually use the 555 prefix for phone numbers.) When I told the IRS person they would probably get lots of phone calls, they did not sound very happy.

James Zuchelli

[It certainly is a departure from the usual 555 regime. But what is interesting is that the number is now permanently problematic, as VCRs

will go on forever with that number. PGN]

## ✓ Greening of Computers

Mark J. Crosbie <mcrosbie@unix1.tcd.ie> Tue, 15 Sep 92 11:52:18 +0100

Re: PC board waste in San Francisco Bay (Agre, RISKS-13.79),

In a similar vein, this month's (Sept.) issue of Byte has an article on the "Greening of Computers". It certainly opened my eyes to the various issues involved when disposing of computer hardware.

I wonder if there would be a call for a newsgroup to discuss these environmental issues in relation to computers (including, I suppose, research into the adverse effects of over-exposure to monitor radiation etc.) as against comp.risks which discusses hardware/software failures and such like.

The group would take into account the more wide-ranging impact of computing on the environment as a whole, and also discussions of methods of minimising the harmful effects could take place.

If it already exists, what is it called, if it doesn't would comp.risks.environmental would be a good name for it? Does this entail a call for votes to set it up??

Any ideas, takers, or comments???

Mark Crosbie, Dept. of Computer Science, Trinity College, Dublin, Dublin 2 IRELAND. mcrosbie@vax1.tcd.ie

[RISKS is certainly a good place for technology related environmental issues. PGN]

### Michigan Awarded Funds to Improve Criminal History Records

Nigel Allen <Nigel.Allen@lambada.oit.unc.edu> Tue, 15 Sep 1992 23:03:06 GMT

After someone mentioned problems with incorrect information about outstanding arrest warrants in police databases, I thought I should mention that the U.S. Justice Department is awarding state governments grants to improve their criminal history databases.

The following press release from the U.S. Justice Department is typical of the announcements it makes when it announces a grant to a state government.

Michigan Awarded Funds to Improve Criminal History Records To: Michigan Correspondents Contact: Stu Smith of the Office of Justice Programs, U.S. Department of Justice, 202-307-0784 or 301-983-9354 (after hours)

WASHINGTON, Sept. 9 -- The U.S. Department of Justice has awarded Michigan \$50,000 to continue improving the quality of the state's criminal history recordkeeping, the Bureau of Justice Statistics (BJS) announced today.

The project, administered by BJS in the Office of Justice Programs (OJP), is part of a three-year, \$27 million Criminal History Record Improvement (CHRI) program established by the attorney general to help states upgrade current systems used to maintain records of arrests, prosecutions, convictions and sentences. The Bureau of Justice Assistance is providing the funding through the Edward Byrne Memorial State and Local Law Enforcement Assistance Program.

"The major objective of this cooperative agreement is to improve the overall quality of the state's criminal history record information by improving disposition reporting," said BJS Director Steven D. Dillingham. "This administration is making every effort to assure the highest standards of accuracy and timeliness in criminal history record information across the country. "It is critical that law enforcement officers, prosecutors, judges and corrections officials have access to complete and accurate information on each individual within the purview of the criminal justice system," Dillingham commented.

The Michigan State Police will use the assistance to identify, retrieve and enter missing court disposition records and develop an automated court records system.

"The program emphasizes the recording of arrest, conviction and sentencing information in a form that will make felony history information more reliable and complete," Dillingham commented. "This is a crucial component of the overall objective of insuring that state criminal history records are up-to-date and available to all criminal justice agencies."

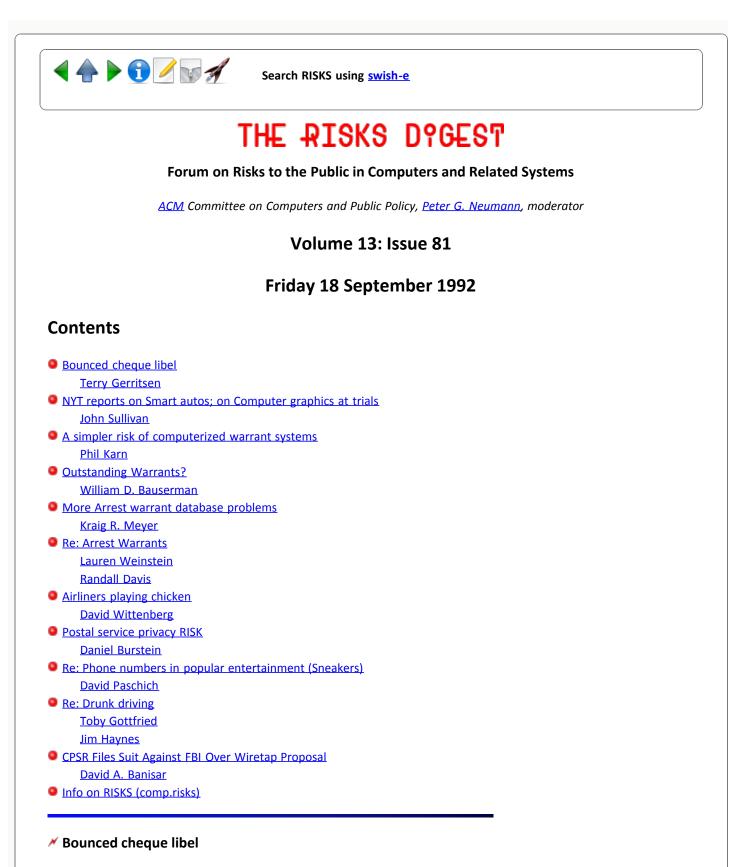
Additional information about this program is available from BJS. Publications and statistical and research data may be obtained from the National Criminal Justice Reference Service, Box 6000, Rockville, Md. 20850. The telephone number is 1-301-251-5500. The toll-free number is 1-800-732-3277.

> internet: bbs.oit.unc.edu or 152.2.22.80 [rampant disclaimers deleted. All are in effect.]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Terry Gerritsen <terry@gtm-inc.com> Sat Sep 19 21:02:45 1992

SPALDING, England - -In what is being hailed as a landmark decision, a bank that mistakenly bounced a client's cheques will pay more than 50,000 pounds in libel damages, a British court has ruled. The July decision from the High Court concluded a nine-year legal battle between Brian and Margaret Allen, operators of a Lincolnshire meat firm, and Llyods Bank.

The conflict began in 1983 when several cheques from the Allen's company were returned by the bank unpaid and marked "Refer to drawer, please re-present," even though there were sufficient funds in the account to cover them. The Allen's counsel, Micheal Tugendhat, said that the couple took the bank to court because they wanted to "eradicate publicly any doubt about their financial soundness and credit worthiness" created by the error.

The libel case is believed to be the first of its kind to reach British courts in this century. Expert Mark Stephens commented that the problem is common but "very few people, including lawyers, are aware that it amounts to libel. The suggestion is that someone issued a cheque knowing he had insufficient funds to meet it, and that can be a very serious libel.

(The Lawyers Weekly)

Terry Gerritsen, G.T.M. Incorporated, Kingston, Ontario(613) 384 0162terry@gtm-inc.comFax: (613) 389 4594

### MYT reports on Smart autos; on Computer graphics at trials

<sullivan@geom.umn.edu> Thu, 17 Sep 92 12:01:21 CDT

The New York Times business section for Sun 6 Sep 1992 had an article on Forensic Animation, using computer graphics reconstructions of events as trial evidence. Lawyers seem enthusiastic, because this will entertain the jury. One (who lost his case) said jury members told him afterwards that they liked the "cartoons".

There have been challenges to the use of such animations. In one murder trial, the defendant said he thought the victim had a raised gun in his hands. The prosecution's animation showed a [stick?] figure of the victim walking with arms down, but the judge only let that segment be shown with the victim "represented by a gray dot".

A Houston lawyer is quoted as saying that once one side has an animation, the other side "starts scrambling" to get its own, since "they are so taken with" the idea. Thus they don't tend to challenge the animations.

The Sun 13 Sep business section has a short note on computer backups during Hurricane Andrew at Grand Met's Miami computer center. These are presented as quite successful, though I was surprised that this involved spending 8 hours making tape backups, hiding them while the storm came through, and then flying them out by helicopter once it had passed.

This issue (13Sep) also has a long article on "intelligent cars", discussing infrared vision systems for night driving, an "autonomous" cruise control, and collision avoidance. These are being investigated by the European Prometheus project, and the article reports on tests made by Jaguar.

The infrared image would be displayed on a CRT or on a heads-up display on the windshield. The new cruise control would attempt to keep two seconds behind another car. Developers (at the British firm Lucas Automotive) say they chose not to give it the ability to apply the brakes fully, so as not to scare drivers. But they hope that "once people trust the computers to operate the various functions on the car for them, they will then allow the computer to do more for them in the future".

They do seem to be paying attention to the fact that (unlike fighter pilots) drivers of these cars will not be specially trained: "the average guy must drive the vehicle". Thus "company secretaries" have been testing the cars at Jaguar.

The collision avoidance system is envisioned at the moment as only providing warnings, not actually interfering with the driver. It might be able to warn drivers who are dozing off.

The Europeans hope to have these systems available within 5 or 10 years; American car companies admit they are a bit behind "because of all the government subsidizing" in Europe.

-John Sullivan, The Geometry Center, Univ of Minnesota sullivan@geom.umn.edu

## A simpler risk of computerized warrant systems

Phil Karn <karn@servo.Qualcomm.COM> Sat, 19 Sep 92 16:49:26 -0700

There's another risk associated with these new computerized warrant systems, at least when they're installed in police cars where they can be used by the drivers.

An exhibit at the San Diego Computer Fair features a police car equipped with a new MDT (Mobile Data Terminal). They're about a year old, and are now in just about every marked San Diego police car. It consists of a specialized keyboard and display mounted to the right of the driver. It allows the user to run license plates and drivers licenses, check for warrants, etc. The system also allows for routine communications, such as checking in and out of service, car-to-car chatting, etc. It can be used for emergency communications such as ordering ambulances, but the officer said that voice was usually quicker for such things. There is, however, a prominent button labeled "EMERGENCY".

The equipment was on a swivel mount so it can be used by anyone in the front seat. When I saw it, it was turned to the left so the driver could use it. I asked the officer demonstrating the system whether there was any official policy on the driver's use of the terminal while in motion. He said the only policy so far was to "use the minimum number of keystrokes necessary" while in motion. And, he added with a wry smile, if you have an accident while using it, then by definition you've just exceeded the minimum number of keystrokes necessary. When I pressed him a little further, he admitted to having had a few close calls already.

Because the system is so fast and easy to use, the officers run plates with it much more often than when they had to do it by voice. So instead of calling in a request only when they really suspect somebody (e.g., during a stop), they like to drive around semi-continuously punching in license plate numbers. Car-to-car chatting also seems to be popular. Although things will probably improve as the novelty of the system wears off, the safety risk here should be fairly obvious.

Phil

### ✓ Outstanding Warrants?

<WILLIAM.D.BAUSERMAN@gte.sprint.com> 21 Sep 92 20:19:00 UT

The recent postings on outstanding warrants reminded me of a problem a friend of mine had about a year ago. This friend owns several wholesale outlets and must travel quite often to procure stock. Because of this frequent travel, he had a tendency to become "lead-footed" and as a result he had quite a few speeding tickets.

To make a long story short, a letter from the Roanoke (VA) Police Department arrived at his house one day while he was out of town on business. The letter was addressed to both him and his wife, and since he had not told her he had been to Roanoke in the last few years, she had to open it.

The letter basically asked them to come to Roanoke and turn themselves in for hit and run (their van had been seen leaving the accident). Well, since, she had not been to Roanoke the mess hit the fan when he got home. When he finally calmed her down enough to believe that he had not been to Roanoke, they called the police.

What they discovered was that, yes there had been a hit and run accident in Roanoke, but the only information the eyewitness could give was that the vehicle was a blue Chevy Astro with license plates AR?-???. Since this was the only lead they had, they pulled the DMV records for all the vans that fit this description and mailed them all a letter. Because he could provide a ironclad alibit the matter was dropped at this point.

But what if he couldn't provide an alibi or what if he had really been in Roanoke but still didn't commit hit and run. I imagine it could have been pretty ugly - if not with the police at least with his wife!

william.d.bauserman@gte.sprint.com

### More Arrest warrant database problems (Hanlon, <u>RISKS-13.79</u>)

<kmeyer@aero.org> Wed, 23 Sep 92 13:16:05 PDT

In <u>RISKS 13.79</u>, James Hanlon mentions the problem of people being detained by law enforcement officials because of incorrect or outdated arrest warrants.

This apparently is a big problem in California, at least in Southern California. In my two years at college in Los Angeles, I knew two people who were erroneously taken in by the LAPD after being pulled over for routine traffic violations (speeding, etc).

A fairly common cause for this may be the traffic school system. In California, if you get a traffic ticket you can usually go to traffic school rather than just pleading guilty and paying your fine. However, if you don't either go to traffic school or pay your fine, eventually the ticket triggers an arrest warrant. My traffic school instructor specifically told us to keep our traffic school completion certificates in our glove compartments for 7 years or there was a reasonably good chance that we'd get hauled down to the station next time we were pulled over for a routine traffic violation.

Kraig R. Meyer

### Ke: Arrest Warrants (Hall, <u>RISKS-13.80</u>)

Lauren Weinstein <lauren@cv.vortex.com> Wed, 16 Sep 92 20:19 PDT

Greetings. The phenomenon of "surprise" arrests for "minor" offenses is by no means a new one, but the masses of computerized records have probably exacerbated the problem.

A friend of mine tells how about ten years ago when she was staying at her parent's home, Culver City police showed up unexpectedly at the front door with an arrest warrant. (Culver City is small city completely surrounded by the City of L.A. Its main claim to fame is the number of film studios, including MGM, within its borders). Anyway, they handcuffed this teenager and led her away. Great fun for the neighbors watching.

Why? Turned out she had what they claimed were some unpaid \*parking\* tickets, which shouldn't have been charged against her in any case since she was a resident of the area who was supposed to be "immune" from that ticketing. The judge they brought her before immediately dismissed them all, but it was still a very embarrassing episode for her. There's just no telling what will pop out of the machines to "roll on" if it's a "slow" day.

The classic treatment of the "computer-induced" nightmare through "minor" errors must be the humorous (fictional) piece done by "Datamation" in the early 70's. It shows a trail of correspondence between an unfortunate book club member and a wide variety of computerized systems, and tells, with tongue held firmly in cheek, of his unfortunate demise. (A clue: at the end of the piece, the governor's order to stop the execution is accidentally misrouted...)

Lauren

### Ke: Arrest Warrants (Hall, <u>RISKS-13.80</u>)

Randall Davis <davis@ai.mit.edu>

Thu, 17 Sep 92 11:30:18 edt

... (I wonder whether there was any human intervention up to the point where the judge issued the warrant.)

How can you imagine there wasn't any? How did the information get from the bank to the police? Did the bank computer take the initiative to dial up the police computer? How did the police decide to accept the information as valid and initiate the warrant process?

Disclaimer: This story was related to me a few years ago by a former employer. I believe that the facts as I have stated them are essentially correct, though the details are no longer clear in my memory.

The story has a strong tone of urban legend. Many crimes involving money have categories of severity depending on amount. Given the alleged facts here the amount in question must have been on the order of \$3; perhaps someone with knowledge of criminal law can indicate if there is in fact any state in which a crime involving \$3 is a felony. Given that ``looking for him for a while'' had to involve some human action (even to put him on the ``wanted'' list), there was some opportunity for sanity checking; no guarantee of course but unlikely to be missed.

If this happened at all, it's far more likely that some serious sized bad checks were written (perhaps ordinary oversight) just before leaving the state, and the combination of events triggered serious action (as it should). The service charges may also have accumulated, but not caused the problem.

### Airliners playing chicken

"David Wittenberg" <dkw@chaos.cs.brandeis.edu> Tue, 22 Sep 92 14:22:52 EDT

In November (presumably 1991), a Fokker 100, flight 1163 landed on runway 22L at O'Hare. Winds were from 240 at 25 kts. Shortly after landing, they discovered that the thrust reversers weren't working, but the multi-function display unit showed no problems. They then found out that the brakes weren't working either. The stick shaker was on. (A stick shaker literally shakes the yoke to warn that a stall may be imminent.) They took the high speed turnoff onto a taxiway, and then turned back onto runway 22L (going in the other direction, so it could also be called 4 R), just as a United 737 landed on the far end of 22L.

Denny Cunningham described it:

"The UAL 737 had already touched down on 22L and was rolling head on toward the Fokker. [The Controller] immediately issued a go-around to the next arrival, then started a persuasive campaign to convince the pilot of the 737 on rollout that it would be in the best interest of aviation safety to make the highspeed taxiway without delay. With the radome of the Fokker starting to fill his windshield, the 737 pilot concurred in a tone of amazement not usually heard on ATC frequencies. He managed to clear the runway a few seconds before the

Fokker flashed by going in the opposite direction.

The Fokker pilot kept one engine running to provide hydraulic power to the steering. At the end of 22L, he turned onto runway 27L, which was being used for take-offs. The planes which were waiting to takeoff were unable to make any room for the Fokker on the taxiway. At this point there were 3 jets rolling on runway 27L. The tower said that it looked like Oshkosh for airliners. The plane just starting its takeoff roll rushed his takeoff to get out of the way. The Fokker finally stopped in the middle of runway 27L, and was towed off safely. Noone was hurt, and there was no damage to any of the airplanes.

It turns out that the "squat" switch which determines if the plane is in the air had jammed, so the plane "thought" it was in the air, and safety switches prevented the brakes or thrust reversers from working while the plane was in the air.

Shortly after this incident, a captain attended school on Fokker 100s and asked what the appropriate procedure was in the event of malfunctioning ground/flight switches. He was told that there wer no such procedures, because it couldn't happen.

This is excerpted from two articles in "IFR: The Magazine for the Accomplished Pilot", Vol. 8, number 9 (sept. 92). They were published under the title "EEK! No Brakes! Ho Hum, just another day at O'Hare; Two airliners playing chicken on runway 22L" "Cockpit View" by Joseph J Poset taken from the May issue of "Airline Pilot", and "From the Tower" by Denny Cunningham.

This incident was not directly caused by a computer. Switches are used in all sorts of safety devices, both with and without computers. The danger from computers is that they tempt us to add many more such switches, which will eventually fail.

In case anyone is tempted to say that safety features such as the one which prevented the brakes from working should be removed, remember that they are often crucial. The opposite kind of accident happened on 5 July, 1970 near Malton Airport in Toronto, where a DC-8 crew accidentally deployed the aircraft's spoilers in flight, killing all aboard. The (US) FAA then required a placard reading "DEPLOYMENT IN FLIGHT PROHIBITED" over the spoiler lever. A Canadian official called this ridiculous, and instead proposed a placard reading "DO NOT CRASH THIS PLANE". In fact the placard did not prevent a similar (but non-fatal) accident on 23 June, 1973 at JFK.

So, placards don't work, and we install safety devices to prevent people from doing stupid things. Then the safety devices fail and cause crashes. All one can do is to try to only add safety devices which help more often than they do damage, and not panic when a safety device does cause damage. We know that will happen, despite all attempts to reduce the frequency.

### postal service privacy RISK

Daniel Burstein <0001964967@mcimail.com>

#### Fri, 18 Sep 92 05:49 GMT

There have been quite a few articles discussing the privacy aspects (or lack thereof), based on the US Postal Service's databases - especially the "forwarding" system.

The following article, from "Labor Notes" (7435 Michigan Avenue, Detroit, Mich. 48210, (313) 842-6262) #160, July 1992, is targeted towards labor issues, but people reading this Digest will quickly grasp the RISKS involved with videotaping all postal envelopes. (see additional comments added at end).

-----

Title: Fighting Privatization. Postal workers urge campaign to organize the new, private sector, mailing industry, by Sarah Ryan

Text: If top US Postal Service officials have their way, private corporations will sort most of the mail by the mid 1990s. And the jobs will pay little better than minimum wage.

But some members of the American Postal Workers Union are hoping to block management's plan with an organizing drive in the private sector mailing industry. A resolution will be presented to the August APWU national convention would, if passed, require the union, which has until now included only governmentemployees, to begin to organize workers in privately-held automated mail processing plants.

Over 40,000 postal union jobs have been eliminated in the last two and a half years, and at least 55,000 more are slated to go by 1995. While many postal workers and union officials believe they are losing jobs to "automation," postal work is being pushed into the hands of an alternate, privately-owned, mailing industry.

Management calls the process "worksharing." Contractors are eager to jump into mail processing and take advantage of the extremely low wages, absence of unions, new high-speed mail processing equipment, and public subsidies.

#### subtitle: Worksharing

A year ago USPS announced that the new Remote Video Encoding operation would be contracted out. Remote encoding was developed as a way to sort mail which cannot be "read" by optical character readers and bar code sorting machines. RVE also allows mail to be sorted without highly trained workers.

Some mail, such as handwritten letters, cannot now be read by machines. The new process will transmit the image of these letters through telephone lines to a data entry operator at a video terminal. The worker enters an extract code, and a bar code is chosen by computer and applied to the letter. The operator can be thousands of miles away from the mail.

According to former Postmaster General Anthony Frank, the remote video operation will eventually replace most to the nation's 49,000 mechanical letter sorting machine jobs. Over 200 remote keying sites are planned; the first ones are already on line.

[the article then goes on to discuss the various financial incentives being proposed by the USPS -and- local governments for the companies setting up these remote operations. It also compares the salaries for the workers. Other tidbits in the piece describe some specific labor issues, use of convicts by the USPS, and the like)

-----

Added comments: No doubt the first few machines will only be used for sorting and bar-code spraying handwritten addresses. HOWEVER, given OCR technology, it would be quite trivial to have EVERY piece of correspondence going through the USPS scanned, and a data list of who sent what to whom could be generated.

I can't cite the reference this moment, but I'm pretty sure the courts have ruled that "mail covers" are legal WITHOUT a search warrant. In other words, "they" can look at the return addresses on the letters in your mailbox (or the addresses you send "to") without legal hassles. (Contents, though, are protected, a little...)

Seems it may be time to change some laws... <dburstein@mcimail.com>

## Phone numbers in popular entertainment (was Re: Sneakers, the movie)

<dpassage@postgres.berkeley.edu> Wed, 16 Sep 92 22:38:14 PDT

In <u>RISKS-13.80</u>, James Zuchelli points out that the movie <u>Sneakers</u> used a real phone number, that of the East Bay IRS office, instead of the normal 555-xxxx used in movies an on TV. PGN then points out that the phone number will be more or less useless for the rest of time because people will be watching the movie on videotape.

On a similar vein, I'm sure lots of the RISKS readers are familiar with Douglas Adams' \_The Hitchhikers Guide to the Galaxy\_, in which a phone number appears and is identified as such early on in the book. The number is the real phone number of the flat in London in which Adams lived while writing the radio series which the book is based on. An introduction to a later collection of Adams' books contained an exhortation not to call the number, as the people currently living there have nothing to do with the book and really wish people would quit calling them up.

I think this brings up an interesting issue as we move into an era in which people are identified on the net by their account names and site. We've all heard of incidents where one person's credit record gets confused with that belonging to another person with the same name. The main student system here has recycled several account names as older students graduate and new students with the same name show up, request an account with the now freed name, and inherit that person's net reputation and hate mail.

**David Paschich** 

## Ke: Drunk driving (Haynes, <u>RISKS-13.80</u>)

Toby Gottfried <toby@felix.filenet.com> Fri, 18 Sep 92 09:51:08 PDT

[The following message, although drifting in RISKS-relevance, is brought to you as a public service. Good advice. PGN]

Advice to (responsible) drivers is: don't drink. If you are arrested for DUI, you'll have full confidence in passing any test by a wide enough margin to avoid worrying about the minor inaccuracies of any machine.

If you know you are guilty, then be thankful that you were stopped before something serious happened. The RISKS are to life, limb, and property, not the passing or failing of a breathalyzer test.

Drivers are tasked with safe driving, not seeing how close they can come to getting away with anything.

I apologize if this is off the subject of computer risks, but I tried and was unable to let Jim Haynes' last paragraph go unanswered.

## Ke: Drunk driving (Gottfried, <u>RISKS-13.81</u>)

Jim Haynes <haynes@cats.UCSC.EDU> Fri, 18 Sep 92 11:35:09 -0700

Well, I agree - I druther people didn't drink at all when they drive, and when I gave that advice it was with misgivings that it might be construed as "how to beat the test" rather than scientific advice. I was being a little tongue-in-cheek when I said take the test and fight the results in court -meaning only to say the machine isn't infallible. I was trying to say with a little bit of humor that you shouldn't risk your future on a breath test when there are better tests available.

# ✓ CPSR Files Suit Against FBI Over Wiretap Proposal

David A. Banisar <Banisar@.cpsr.org> Thu, 17 Sep 1992 16:43:51 -0400

WASHINGTON, DC, September 17, 1992

Contact:

Marc Rotenberg, CPSR Director (202/544-9240) rotenberg@washofc.cpsr.org David Sobel, CPSR Legal Counsel (202/544-9240) sobel@washofc.cpsr.org CPSR Sues FBI For Information About Wiretap Proposal: Seeks Reasons for New Plan

Washington, DC - Computer Professional for Social Responsibility filed suit today against the FBI for information about a new wiretap proposal. The proposal would expand FBI wiretap power and give the Bureau authority to set technical standards for the computer and communications industry.

The suit was filed after the FBI failed to make the information public. In April, CPSR requested documents from the Bureau about the reasons for the proposal. The FBI denied that any information existed. But when CPSR pursued the matter with the Department of Justice, the Bureau conceded that it had the information. Now CPSR is trying to force the Bureau to disclose the records.

The proposal expands the FBI's ability to intercept communications. It would mandate that every communication system in the United States have a built-in "remote monitoring" capability to make wiretap easier. The proposal covers all communication equipment from office phone systems to advanced computer networks. Companies that do not comply face fines of \$10,000 per day.

The proposal is opposed by leading phone companies and computer manufacturers, including AT&T, IBM, and Digital Equipment Corporation. Many charge that the FBI has not been adequately forthcoming about the need for the legislation.

According to CPSR Washington Office director Marc Rotenberg, "A full disclosure of the reasons for this proposal is necessary. The FBI simply cannot put forward such a sweeping recommendation, keep important documents secret, and expect the public to sign off."

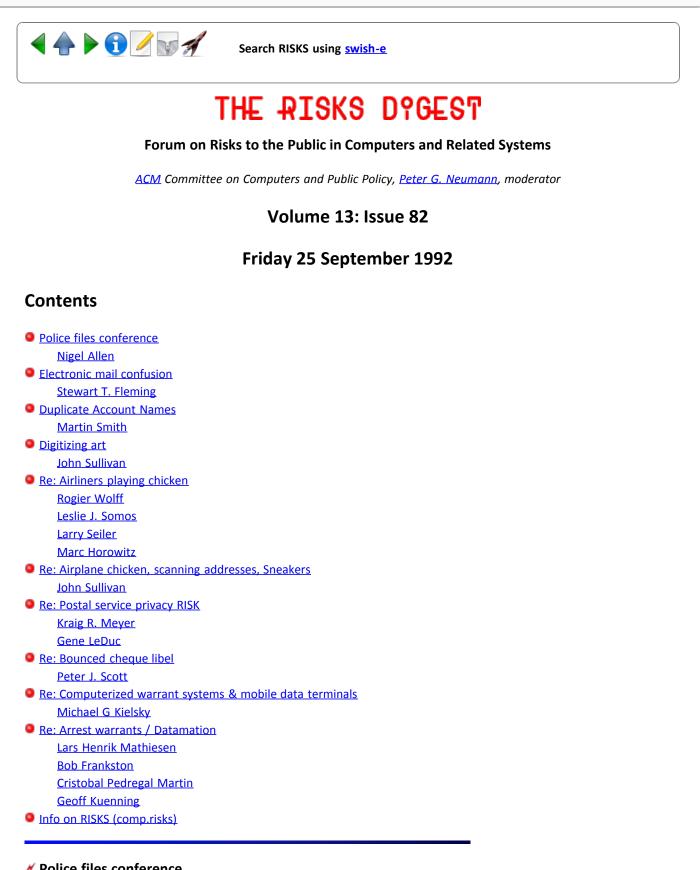
In a related effort, a 1989 CPSR FOIA suit uncovered evidence that the FBI established procedures to monitor computer bulletin boards in 1982.

CPSR is a national membership organization of computer professionals with over 2,500 members based in Palo Alto, California with offices in Washington, DC and Cambridge, Massachusetts and chapters in over a dozen metropolitan areas across the nation. For membership information, please contact CPSR, P.O. Box 717, Palo Alto, CA 94303, (415) 322-3778, cpsr@csli.stanford.edu.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



# Police files conference

Nigel Allen <nigel.allen@canrem.com> Tue, 22 Sep 1992 20:00:00 -0400

Here is a press release from the U.S. Department of Justice.
National Criminal Justice Information Conference in New Orleans
To: City and Assignment desks
Contact: Stu Smith of the Office of Justice Programs,
U.S. Department of Justice, 202-307-0784 or

301-983-9354 (after hours)

WASHINGTON, Sept. 23 -- A national conference on federal-state criminal justice information sharing will be held from Wednesday, Sept. 23, through Saturday, Sept. 26, in New Orleans, the Department of Justice announced today.

Jointly sponsored by the Bureau of Justice Statistics (BJS) and the Justice Research and Statistics Association (JRSA), the conference participants will discuss "Federal and State Information Sharing to Effectively Combat Crime and Ensure Justice."

Specific topics that will be aired include "New Measures in the Criminal Justice System," "Weed and Seed' and New Drug and Crime Prevention Initiatives," "Challenges and Reforms to the Justice System in the 90s," "Uses of Incident-based Reporting Systems," "Recent Developments in Criminal History Improvements" and various research issues in corrections, prosecution and law enforcement. Among the approximately 250 people expected to attend will be officials from state and local government and various federal agencies as well as leading criminal justice researchers and scholars. Other participants will be the directors of State Statistical Analysis Centers (SACs) and other members, associate members and guests of JRSA.

BJS has provided funding to state justice statistics and information systems through a network of SACs since 1972. There are currently SACs in 48 states, the District of Columbia, Puerto Rico, the Virgin Islands, and the Northern Mariana Islands. The SACs provide a wealth of data about crime and the operation of the criminal justice system to state and local governments, legislatures, and Attorneys General for policy analysis and planning purposes.

This year is the 20th anniversary of the SAC program. It also marks the beginning of a new initiative to establish a truly national system of federal, state and local government information-sharing and readily accessible data bases.

Additional information about BJS programs and publications may be obtained from the Bureau of Justice Statistics Clearinghouse, Box 6000, Rockville, Md. 20850. The telephone number is 800-732-3277.

Canada Remote Systems - Toronto, Ontario World's Largest PCBOARD System - 416-629-7000/629-7044

### Electronic mail confusion

"Stewart T. Fleming" <sfleming@cs.heriot-watt.ac.uk> Thu, 24 Sep 92 16:27:17 +0100

I wasn't going to contribute this until I read David Paschich's contribution (Wed, 16 Sep 1992) concerning potential confusion of users on electronic networks.

Working within a computer-oriented university department, a lot of internal work (memos, reminders etc) gets distributed by e-mail. Such distribution

lists exist for staff, postgraduate students and so on. This afternoon, a postgrad. student was surprised to receive complaints from postgraduates at a neighbouring institution about an e-mail message he had sent for internal distribution.

What had happened was that an electronic mail address had become truncated and passed through the smart address matching path. None of the machines on that path flagged the address as invalid and the mail was sent on up the chain. When it reached the other institution, it was distributed to their postgraduates.

This incident illustrates the potential for embarrassing disclosures, particularly in view of two results from a recent e-mail survey we carried out:

- Q: Have you sent or received confidential/sensitive information by electronic mail ?
   Yes: 75%
- Q: Was the material encrypted or protected in any way ? No: 91%

Do you know where your e-mail messages are ? STF

sfleming@uk.ac.hw.cs or sfleming@cs.hw.ac.uk or ...uknet!cs.hw.ac.uk!sfleming

### ✓ Duplicate Account Names (was Phone Numbers In Popular Entertainment)

msmith <msmith@lssec.bt.co.uk> Thu, 24 Sep 1992 08:49:21 +0100

David Paschich writes in <u>Risks 13.81</u> about one of the risks of getting account names mixed up, the fact that you could inherit someone's reputation (good or bad).

While at University I came across another aspect of this problem. When people left their accounts were put on tape and deleted. I have a fairly common name (ask Douglas Adams) and there was someone in the year above me also called Martin Smith. Account names were normally first name and initial of surname but their account wasn't called MartinS, presumably because there'd been a name clash in the past. Thus I was known as MartinS.

I came back from the summer holiday and guess which account had been deleted?

Things then became even more confusing when I went to get my files back. There was \*another\* Martin S\* (the surname escapes me) just arrived in the new intake who had already been given my old account name. My account had to be renamed to MartinSm.

I can't help wondering who got deleted when I left.

(not necessarily THE) Martin Smith

### 🗡 Digitizing art

<sullivan@geom.umn.edu> Tue, 22 Sep 92 12:39:37 CDT

The Economist (Aug 15) reports that the National Galleries in both Washington and London have plans to digitally record images of all their paintings, because digital images "last for ever". London hopes to scan their pictures "repeatedly over time ... to track how their colours change": "Since human colour memory is poor, and photographs change colour themselves, the only way to do this is by using a computer."

I have trouble here dealing with image files I created a couple of years ago: we have new hardware, software, and file formats. I have all but given up hope that colors will look similar on the screen, when printed, and when scanned in. I hope the museums will give careful thought to such problems.

-John Sullivan, The Geometry Center, University of Minnesota

### Ke: Airliners playing chicken

Rogier Wolff <wolff@zen.et.tudelft.nl> Thu, 24 Sep 1992 12:19:50 GMT

Last time I heard about this incident (Here on comp.risks I believe) it was told that \_both\_ "squats" had failed. I.e. there where considerations towards reliability and safety of the devices.

An interesting question pops up now. Should these devices be wired in an "and" or in an "or" fashion? I guess that it would be safest to wire them in such a way that when they agree, they can override the pilot, but if they disagree, the pilot should be able to take responsibility.

Roger

EMail: wolff@duteca.et.tudelft.nl \*\* Tel +31-15-783644 or +31-15-142371

### Ke: Airliners playing chicken (<u>RISKS-13.81</u>)

Leslie J. Somos <ah739@cleveland.freenet.edu> Thu, 24 Sep 92 10:27:48 -0400

I know nothing about planes.

I can understand preventing deployment of spoilers or thrust reversers while in the air, but I don't understand preventing brake application.

Leslie J. Somos ah739@cleveland.Freenet.edu

### Safety interlocks that fail

LARRY SEILER, DTN225-4077, HL2-1/J12 <seiler@rgb.enet.dec.com> Fri, 25 Sep 92 09:09:53 -0700

re "Airliners playing chicken" from <u>RISKS digest 13.81</u>:

I agree that it is better to have an occasional accident due to a safety interlock system that fails than to have more accidents due to people accidentally doing fatal things like engaging the thrust reversers or deploying the spoilers while the plane is in the air.

However, the better solution is to have an emergency override system that is simple enough to engage quickly, that cannot easily be engaged by accident and that warns that it is engaged. And, of course, there must be severe penalties for anyone who uses it except under emergency conditions.

To use a computer analogy, there can be serious accidents if everyone has superuser privileges enabled all the time. But there are also problems if you cannot get privileges when you really need them -- like at 9pm when no one is around and you just have to read that protected file!

Larry

### Ke: Airliners playing chicken

Marc Horowitz <marc@Athena.MIT.EDU> Wed, 23 Sep 92 22:54:47 EDT

Or, we can realize that failures and "impossible" circumstances do occur, and install overrides so the pilot can tell the system it's wrong. People deal with unforeseen circumstances better than computers.

Marc

### Airplane chicken, scanning addresses, Sneakers

<sullivan@geom.umn.edu> Thu, 24 Sep 92 16:04:47 CDT

A few quick comments on items in **RISKS-13.81**:

David Wittenberg reports on airliners playing chicken, and suggests that we "not panic when a safety device does cause damage" even though switches "used in all sorts of safety devices ... will eventually fail". I'd like to see an overridable switch: if the pilot engages the brakes or thrust reversers, and the computer thinks the plane is in the air, it shouldn't just quietly fail to engage them, but should tell the pilot what is going on, and leave some way to override the ground/flight switch.

Daniel Burstein is concerned about the post office's plans to send images of hand-written envelopes via computer to remote sorting sites, and the possibility that addresses could be stored in a database. Of course letters with typed addresses are already sorted by machines with OCR software, so these addresses are even easier to store. Overnight delivery services must enter each item sent into some kind of computerized tracking and billing system: who knows if any of them have thought to keep a database indexed by sender/recipient pairs?

There has been much discussion of the real phone number used in 'Sneakers' for the NSA agent. The movie also shows phone numbers being typed in on a numeric keypad (when they first test the decoder), and at least one instance where touchtones are audible. I didn't try to identify any of these, but I'm sure someone will.

-John Sullivan, The Geometry Center, Univ. of Minn. sullivan@geom.umn.edu

### Re: postal service privacy RISK (<u>RISKS-13.81</u>)

<kmeyer@aero.org> Thu, 24 Sep 92 14:28:07 PDT

In <u>RISKS-13.81</u>, Daniel Burstein relays US Postal Service plans to use remote video technology to allow remote sorting of mail, and notes: "given OCR technology, it would be quite trivial to have EVERY piece of correspondence going through the USPS scanned, and a data list of who sent what to whom could be generated."

I want to point out several issues related to this article:

1. The RISK of stored communication matrices--having a record of who communicates with whom--is perhaps simplified, but certainly not created by the use of computer sorting technologies. In small town days, the local postman and telephone operator knew exactly who communicated with whom.

2. OCR Technology is already very widely used by the USPS. If you place a letter in a mailbox that is designated "for envelopes with typed and printed addresses only," that envelope is read by an OCR and a bar code is put on to the envelope corresponding to the zip code. (Try sending yourself a letter in this manner!)

3. There was a front-page article in the LA Times (Sunday, 20 Sept?) that describes how firms in general are using remote technologies to move jobs to remote locations. It's generally a benefit to both the company and the workers. The company gets better workers and lower costs. The workers are happier because their wages go a lot further in the remote geographic location, allowing a better standard of living. Why not let workers in Vermont sort mail that is going through a plant in New York City?

### Re: postal service privacy RISK (<u>RISKS-13.81</u>)

LCDR Gene LeDuc <leduc@nprdc.navy.mil>

### Fri, 25 Sep 92 07:33:53 PDT

In <u>RISKS-13.81</u> Daniel Burstein wrote about Remote Video Encoding in use by the USPS, a procedure involving scanning a letter and sending the envelope's image to a remote site to be ZIP and barcode processed. [...]

Those who fear this type of data collection are certainly under no obligation to include a return address on any envelope. In this case (for once!), the default in mailing a letter is "no return address" and one must override this default by putting one on the envelope.

-gene-

Gene LeDuc (leduc@nprdc.navy.mil), Navy Personnel R & D Center, San Diego, CA 92152-6800

### Ke: Bounced cheque libel

Peter J. Scott <pjs@euclid.JPL.NASA.GOV> Wed, 23 Sep 92 16:53:44 -0700

Terry Gerritsen quotes The Lawyers Weekly as saying that the 9-year libel action, ultimately successful, of a company against Lloyd's bank for erroneously returning cheques marked "Refer to drawer", is believed to be the first of its kind to reach British courts this century. Actually I am aware of a case identical in all pertinent respects, and while I do not remember the date I am reasonably certain it was within this century. I remember finding it in a search of important libel decisions when I was in the UK and it stuck in my mind. Given such a clear precedent, it's appalling that it took nine years to come to a decision.

Peter J. Scott, Member of Technical Staff | pjs@euclid.jpl.nasa.gov Jet Propulsion Laboratory, NASA/Caltech | SPAN: GROUCH::PJS

### Ke: Computerized warrant systems & mobile data terminals

MICHAEL G KIELSKY <MKIELSKY@apsc.com> Thu, 24 Sep 92 10:47:38 MST

Mobile data terminals (MDT's) in police cars are nothing new around here (Phoenix, AZ area), and have been in use for years. My experience has ranged from working for an organization which serviced these devices (and thus using them in testing), thoroughly studying the computer system that works in the background, to accompanying on-duty police officers from various departments on many ride-alongs, and viewing the system in action. These systems are in use with virtually every police agency in the Phoenix area, as well as the Department of Public Safety (Highway Patrol), but not with the sheriff's office.

The systems are nothing more than data terminals on a radio network. Data traffic is NOT encrypted (risks obvious), and converting an installed base to handle encryption is not feasible for most departments. Log on practices vary,

with identification information ranging from officer ID, to shift/beat code, with usually short (and few different) passwords. The "base computer" is connected to several databases, including the National Crime Information Computer (NCIC), the Arizona Crime Information Computer (ACIC), and motor vehicle records. Information retrievable includes driving license records (including traffic violation history), vehicle registration records (including vehicle description), arrest warrant information, stolen motor vehicle records, stolen firearm records, etc. Data retrieval is notoriously slow during busy times (Friday & Saturday night), sometimes taking as long as 30 minutes for a license plate check. Terminal to terminal messaging is possible. Communication with dispatchers is also possible. All transactions are recorded/printed.

Accident Risks: A few years ago, the Phoenix Police Department, after experiencing numerous problems with officer's driving and operating the terminals at the same time, improved the ergonomics by mounting the terminal higher and closer to the driver. This way, the drivers eyes are not completely averted from the road while using the terminal.

Privacy Risks: It is common practice for officers to "run" license plates on vehicles which they observe, for no reason whatsoever, or for any trivial reason. Information retrieved via the computer includes name, address, SSN, and driving license number of the current registered owner, vehicle identification number, lien holder (usually bank/loan institution), original lien amount, date vehicle first registered, date registration expires, vehicle description, and whether the vehicle is stolen. Registration violations are most commonly found this way. As newer officers (who often are less techno-phobe) take to the streets, use of the system is increasing.

False Arrest Risks: Arrest warrant information obtained through the computer (term is "CAPRI Hit") will find the listed individual in handcuffs (i.e. existence of a computer arrest warrant record is sufficient probable cause for arrest). Again, we know how infallible information entered into computers is. These computer warrant records must then be verified against the actual warrant (on paper), before the arrestee can be arraigned (brought before a judge). These warrants are stored in filing cabinets at the sheriff's office of the warrant issuing jurisdiction (here it is the Maricopa County Sheriff's Office, and I have seen the actual filing cabinets stuffed with warrants). This process can be slow, since there are hundreds of thousands of outstanding warrants in these filing cabinets, some going back over half a century.

Michael Kielsky, Arizona Public Service Company, P.O. Box 53999, Phoenix, AZ 85072-3999 602-250-2897 (W) 602-919-0182 (M) ...sunburn!overlord!mkielsky

### Ke: Arrest Warrants (Weinstein, <u>RISKS-13.81</u>)

Lars Henrik Mathiesen <thorinn@diku.dk> Fri, 25 Sep 1992 12:37:16 GMT

Lauren Weinstein writes about the classic treatment of the "computerinduced" nightmare through "minor" errors: > (A clue: at the end of the piece, the governor's order to stop the > execution is accidentally misrouted...)

Actually, the order was to be sent by a special urgent-mail system --- but it was held back because the Governor didn't get it authorized by his supervisor ... (I think I read this short story in a science-fiction collection named \_The Astounding-Analog Reader\_.)

Lars Mathiesen (U of Copenhagen CS Dep) <thorinn@diku.dk> (Humour NOT marked)

### Ke: A simpler risk of computerized warrant systems (Karn, <u>RISKS-13.80</u>)

<Bob\_Frankston@frankston.com> Thu 24 Sep 1992 11:39 -0400

Consumer car phones are already shipping with voice dialing. Extending that to replacing the keyboard by speaking letters as opposed to something as fancy as full word recognition would be straightforward. Given not only the safety risk but the awkwardness of using a keyboard in a car along with the compelling value of using the device while driving, I'd be surprised if voice is not added very soon.

Let's start the timer going and see how long it takes to get the technology deployed.

### Ke: Arrest Warrants (Davis, <u>RISKS-13.81</u>)

Steve Nuchia <steve@nuchat.sccsi.com> Thu, 24 Sep 92 20:34 CDT

>Given the alleged facts here the amount in question must have been >on the order of \$3;

An incident with similar background but (so far) less outrageous conclusion happened to me. Early in my consultancy I had my business checking account at a small bank. Through a bookkeeping error on my part I bounced a check. The check was small, the account was small, the error was small and the overdraft was small.

In what I hope and believe was a complete coincidence, the bank was closed by federal regulators between the time the check was bounced and the time I received notice of it. The check was not honored but the overdraft charge ate up the balance in the account plus a few dollars. Since I couldn't find anybody who had a clue what was going on I just abandoned the account.

The bank was purchased by Texas Commerce Bank, one of the largest in the area. For several months they accrued overdraft charges to my old account because it now had a negative balance. The end result was that they wrote off the account with about \$75 owing and sent me a nice registered letter to the effect that I had "caused a loss" of \$whatever to the bank. The way I see it they made off with the \$12 I had in there when they bought the old bank, but I suspect they could have one of those stealth arrest warrants issued for me by including my case on a list of other "losses" and mailing it to the district attorney.

I also managed to spend a couple of hours in jail once due to a parking ticket that was over five years old. It was legitimate and once I was told about it I vaguely remembered having gotten it, but I had completely forgotten it. The arresting officer could not tell me what I was being charged with at the time of the arrest, which I found pretty offensive. All he knew was that a warrant existed.

What I don't understand is why they can't send out letters to people instead of lying in wait for them and wasting everybody's time. It wasn't like I was going to flee the country over a parking ticket.

Steve Nuchia South Coast Computing Services, Inc. (713) 661-3301

### Ke: A simpler risk of computerized warrant systems (Karn, 13.81)

<pedregal%unreal@cs.umass.edu> Thu, 24 Sep 92 9:43:17 EDT

Phil Karn comments about a computer terminal mounted on San Diego police cars; these devices can be (and are) used by the driver while in motion. He points out the safety risks associated with that (typing/reading while driving).

Karn also mentions that "[the police] like to drive around semi-continuously punching in license plate numbers", i.e., that they check plates in many situations that are not "only when they really suspect somebody (e.g., during a stop)".

So there's a change with respect to the previous situation: now the checks on plates can be (they probably are) stored and can be manipulated much more easily; more such data is gathered; and, more relevant to RISKS, it can be easily matched with location, as police cars (will) have devices that continuously report their location. Of course, if the records exist, they will eventually be used against someone.

This is yet another instance of a common risk: having more and richer data changes the possible uses of such data.

Cristobal Pedregal Martinpedregal@cs.umass.edu (internet)Computer Science DepartmentUMass / Amherst, MA 01003

### Ke: Datamation fiction (Weinstein, <u>RISKS-13.81</u>)

Geoff Kuenning <geoff@itcorp.com> Wed, 23 Sep 92 18:11:30 PDT

Lauren Weinstein writes:

> The classic treatment of the "computer-induced" nightmare through

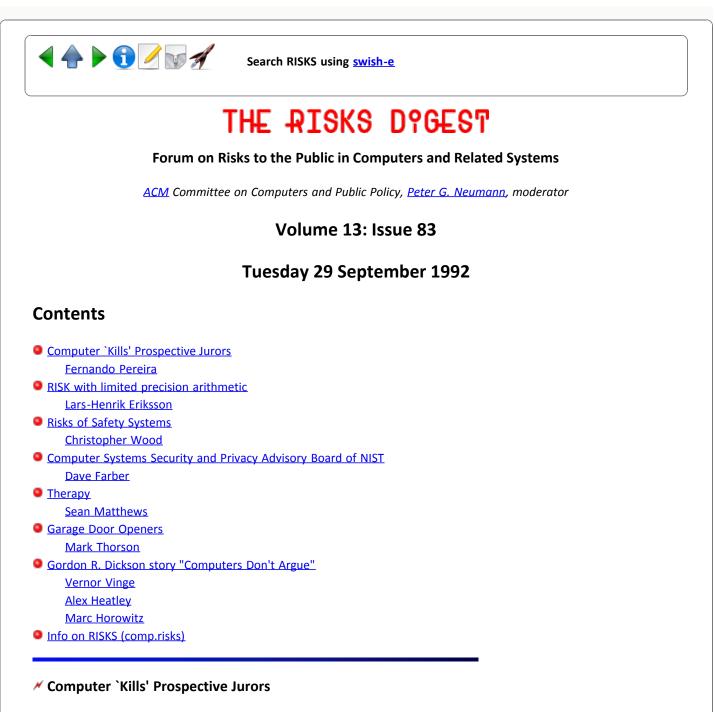
> "minor" errors must be the humorous (fictional) piece done by> "Datamation" in the early 70's.

As I recall, the title of the story was "Computers Don't Argue," and it was not original with Datamation. I think it appeared first as a science-fiction short story in the late 60's.

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff



Report problems with the web pages to the maintainer



Fernando Pereira <pereira@mbeya.research.att.com> Tue, 29 Sep 92 10:20:33 EDT

The Associated Press reports in 9/29 from Hartford, Conn. that for the last three years Hartford residents have been excluded from the federal grand jury pool. The problem was discovered in a lawsuit disputing the racial composition of the federal grand jury that indicted a minority defendant for bail-jumping. Apparently, the city name for Hartford residents had been typed in the wrong place (wrong field?) in computer records, with the effect that the "d" in "Hartford" overflowed into a status field, indicating the named person as deceased.

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave, PO Box 636 Murray Hill, NJ 07974-0636 pereira@research.att.com [Noted by others as well... PGN]

### RISK with limited precision arithmetic

Lars-Henrik Eriksson <lhe@sics.se> Mon, 28 Sep 1992 19:40:11 GMT

My union just sent out a letter to its members containing (among other things), the note:

"If your salary is less than 11844 or greater than 32767, please notify us immediately and we will adjust your membership fee."

The membership fees are dependent on the salary. My salary is higher than the first figure quoted and I already have the maximum fee. So why the request to people with a salary greater than 32767 swedish crowns?

Since 32767 is the greatest integer you can represent in 16 bits with 2's complement arithmetic, I am willing to bet that their computer misrepresents larger salaries. I guess that someone with an income of 33000 crowns (say) are charged the fee for an income of 33000-32767=233 crowns! That would be the minimum fee...

Someone must have noted this, and now they must correct those cases manually...

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263 S-164 28 KISTA, SWEDEN Phone (intn'l): +46 8 752 15 09

### Risks of Safety Systems

wood,christopher <ccw@prefect.cc.bellcore.com> 28 Sep 1992 15:32 EDT

The incident \_was\_ caused by a computer. An automated system was "in the loop" that examined sensor inputs (including the control for the thrust reversers and brakes (and in the other incident, the flaps), and the indication given by the "squat" switch, and decided whether or not to deploy the thrust reversers and the landing wheel brakes. It seems odd to me (but then again, I'm not an engineer designing commercial aircraft) that the squat switch should \_also\_ disable the brakes, which don't seem like they pose a safety hazard if used during flight.

This seems like an area where a cockpit crew needs to be able to explicitly override the safety system. I can imagine a sort-of dialog (not with spoken or even typed words, but by command actions - pulling levers and switches, and so on...)

Crew: deploy thrust reversers

Safety Systems: No. Use of thrust reversers in flight will destroy the aircraft. Crew: Acknowledged. Override safety constraints! Deploy Thrust Reversers NOW!

### [...]

We still put human crews in airliners. Maybe the next step is to admit that the safety systems are fallible, and give crews a way to overcome that fallibility.

There are numerous design issues involved, though. The safety systems are there for a purpose, and the bypass mechanism should have enough restrictions that it is only used in an emergency, rather than as a way of avoiding a routine bother. On the other hand, if the restrictions are too severe, the crew will be unable to override the systems when they have to. At around 200 MPH, a jetliner runs out of runway \_very\_ quickly, and there isn't a lot of time for access codes, or even synchronizing movements of two crew members. Perhaps requiring a lot of paperwork \_after\_ the use of the override system would be appropriate.

### Computer Systems Security and Privacy Advisory Board of NIST TESTIMONY

Dave Farber <farber@central.cis.upenn.edu> Sun, 27 Sep 92 09:24:43 -0400

>From the EFFector 3.05

Following are excerpts from the testimony of Professor David Farber, a member of the EFF Board of Directors, before the Computer Systems Security and Privacy Advisory Board of the National Institute of Standards and Technology (NIST) on September 16, 1992.

Mr. Chairman and Members of the Advisory Board:

My name is David Farber. I am Professor of Computer Science at the University of Pennsylvania and a member of the Board of Directors of the Electronic Frontier Foundation (EFF). I am here today representing only the views of EFF. I want to thank you for inviting us to testify today as part of your investigation.

We are pleased to be included at this early phase of the Advisory Board's inquiry and offer a brief set of principles for proceeding with this inquiry. First, it is essential that in examining discrete issues such as the desirability of various cryptography standards, the Board take a comprehensive view of what we call "digital privacy" policy as a whole. Such a comprehensive view requires a clear vision of the underlying civil liberties issues at stake: privacy and free speech. It also requires looking beyond the cryptography questions raised by many to include some of law enforcement's recent concerns about the pace of digital infrastructure innovation. Second, for the sake of promoting innovation and protecting civil liberties, the Board should bear in mind the principle that computer security policy is fundamentally a concern for domestic, civilian agencies. This principle, as articulated in the Computer Security Act of 1987, can serve as an important guide to the work of this Board.

### A. THE GROWING IMPORTANCE OF DIGITAL PRIVACY TECHNOLOGY

With dramatic increases in reliance on digital media for communications on the part of private individuals, government, and corporations, the need for comprehensive protection of privacy in these media grows. For most in this room, the point seems trite, but the digital communications revolution (which we stand at only the very beginning of), is the key event of which the Advisory Board should take note. As an example, a communication which is carried on paper through the mail system, or over the wire-based public telephone network is relatively secure from random intrusion by others. But the same communication carried over a cellular or other wireless communication system, is vulnerable to being overheard by anyone who has very inexpensive, easy-to-obtain scanning technology.

For the individual who relies on digital communications media, reliable privacy protection cannot be achieved without the protection of robust encryption technology. While legal restrictions on the use of scanners or other technology which might facilitate such invasions of privacy seem to be attractive preventative measures, these are not lasting or comprehensive solutions. We should have a guarantee -- with physics and mathematics, not only with laws -- that we can give ourselves real privacy of personal communications through technical means. Encryption strong enough that even the NSA can't break it. We already know how to do this, but we have not made encryption technology widely available for public use because of public policy barriers.

# B. THE BOARD SHOULD UNDERTAKE A COMPREHENSIVE REVIEW OF DIGITAL PRIVACY ISSUES

Inasmuch as digital privacy policy has broad implications for constitutional rights of free speech and privacy, and for international competitiveness and economic vitality in the information age, these issues must be explored and resolved in an open, civilian policy context. These questions are simply too important to be decided by the national security establishment alone. This principle is central to the Computer Security Act of 1987.1 The structure of the Act, which is the basis for the authority of this Advisory Board, arose, in significant part, from the concern that the national security establishment was exercising undue control over the flow of public information and the use of information technology.2

When considering the law in 1986, the committee asked the question, "whether it is proper for a super-secret agency [the NSA] that operates without public scrutiny to involve itself in domestic activities...?" The answer was a clear no, and the authority for establish computer security policy was vested in NIST (the NBS).

In this context, we need a robust public debate over our

government's continuing heavy-handed efforts to control commercially developed cryptography. It is no secret that throughout the cold war era, the Defense and State Departments and the National Security Agency have used any and all means, including threats of prosecution, control over research, and denial of export licenses to prevent advanced secret coding capabilities from getting into the hands of our adversaries. NSA does this to maximize its ability to intercept and crack all international communications of national security interest.

Now the Cold War is over but the practice continues. In recent years, Lotus, Microsoft, and others have developed or tried to incorporate powerful encryption means into mass market software to enhance the security and privacy of business, financial, and personal communications. In an era of computer crime, sophisticated surveillance technologies, and industrial espionage it is a laudable goal.

Although NSA does not have the authority to interfere with domestic distribution of DSA, RSA, and other encryption packages, its licensing stranglehold over foreign distribution has unfortunate consequences. Domestic firms have been unable to sell competitive security and privacy products in international markets. More important, because the cost of producing two different products is often prohibitive, NSA policy encourages firms to produce a single product for both domestic and worldwide use, resulting in minimal privacy and security for users both here and abroad.

While we all recognize that NSA has legitimate national security concerns in the post cold war era, this is a seriously flawed process. Foreign countries or entities who want to obtain advanced encryption technology can purchase it through intermediaries in the United States or from companies in a host of foreign countries who are not subject to US export restrictions. There is a big, big hole in the national security dike. By taking a page out of the Emperor's New Clothes, NSA opts to act as if the process works by continuing to block export.

In order to get some improvement in mass market encryption, the Software Publishers Association, representing Microsoft, Lotus, and others, had to use the threat of legislation to get NSA to engage in the negotiations that finally led NSA to agree to expedited clearance for the export of RSA encrypting software of limited key lengths. Still, all concede that the agreement does not go far enough and that far more powerful third-party products are commonly available in the US, including the fifteen-year-old US Data Encryption Standard. SPA knows that specifying maximum key lengths offers little long-term security given advances in computer processing power, but was willing to compromise because of NSA's refusal to budge.

Does this kind of policy make any sense in the post Cold War era? Mass market products offer limited security for our citizens and businesses. Determined adversaries can obtain much more powerful products from foreign countries or by purchasing it here in the US. Is the NSA policy of slowing down the pace of encryption use by foreigners and adversaries --even if demonstrable--any longer worth the significant price we pay in terms of failing to meet our own communications privacy and security needs? That is the policy challenge for this Board to address by a frank, open, and inclusive public debate.

C. THE BOARD MUST ADDRESS THE DIGITAL PRIVACY ISSUE IN A COMPREHENSIVE MANNER WHICH REQUIRES CONSIDERING THE FBI'S DIGITAL TELEPHONY PROPOSAL AND ITS IMPLICATIONS.

The public policy debate on electronic privacy issues over the last few years has demonstrated that a comprehensive approach to digital privacy policy cannot be complete without examining both questions regarding the availability of encryption technology, and the corresponding infrastructure issues, such as those raised by the FBI's Digital Telephony Proposal. Attempts to solve one issue without addressing the other is an exercise in irrational policy-making and should be avoided by this Advisory Board.

Last year, the FBI first proposed a "Sense of the Congress" resolution stating that communications firms and computer and communications equipment manufacturers were obligated to provide law enforcement access to the "plain" text of all voice, data, and video communications, including communications using software encryption. The Electronic Frontier Foundation (EFF) played an active and leading role both in opposing such a law and in seeking to find more acceptable means for meeting legitimate law enforcement needs. Because of our advocacy and coalition-building efforts with communications and privacy groups, we were successful in persuading Senate Judiciary Chairman Joseph Biden to remove the Sense of the Congress Resolution from active consideration as part of Omnibus crime legislation last year.

Putting aside its attempt to control the use of encryption systems, this year the FBI has come forward with proposed legislation that would require telephone companies, electronic information providers, and computer and communications equipment manufacturers to seek an FCC "license" or Attorney General "certification" that their technologies are susceptible to electronic surveillance. We are in danger of creating a domestic version of the export control laws for computer and communications technology.

While the FBI claims that neither of this year's proposals address encryption issues, the Bureau has made it clear it plans to return to this issue in the future. The Board needs to hear from the broad coalition made up of telephone companies such as AT&T, computer firms such as IBM, Sun Microsystems, and Lotus Development Corporation, and public interest groups such as the EFF. The EFF will shortly release a white paper representing coalition views on the need for the FBI to explore more realistic, less vague, and potentially onerous policy options for meeting legitimate law enforcement needs.

The resulting multi-front battle being waged about digital privacy creates formidable roadblocks to a final resolution of the policy disputes at issue. Those who seek greater privacy and security cannot trust a settlement on one front, because their victory is likely to be undermined by action on the other issue. And law enforcement and national security concerns cannot be adequately addressed without a sense of the overall solution being proposed on both the encryption and infrastructure fronts. This Advisory Board can play a valuable role for the policy process by conducting a comprehensive review of digital privacy and security policy, with a consideration of both of these sets of issues.

 Pub.L.No. 100-235.
 House Committee On Government Operations, H.R. Rep. No. 99-753, Pt. 2, at 5.

### 🗡 Therapy

"Sean Matthews" <sean@mpi-sb.mpg.de> Sat, 26 Sep 92 16:45:38 +0200

Some papers run personals among the classified ads. The New York Review of Books runs not only personals, but, right above them, therapy ads too. This appeared in the October 8, 1992, edition:

FEELING HELPLESS ABOUT DEPRESSION? Overcoming Depression 2.0 provides computer based cognitive therapy for depression with therapeutic dialogue in everyday language. Created by Kenneth Mark Colby, M.D., Professor of Psychiatry and Biobehavioural Sciences, Emeritus, UCLA. Personal Version (\$199), Professional version (\$499). Malibu Artificial Intelligence Works, 25307 Malibu Rd, CA 90265. 1-800-497-6889.

The risks, to coin a phrase, are obvious. If anyone who happens to live in the 'States followed this up, I would be fascinated to know what exactly this thing is.

Sean Matthews, Max-Planck-Institut fuer Informatik, Im Stadtwald, W-6600 Saarbruecken, Germany +49 681 302 5363 (sean@mpi-sb.mpg.de)

### ✓ Garage Door Openers

<mmm@cup.portal.com> Fri, 18 Sep 92 20:45:16 PDT

With regard to garage door opener security, I recently was asked to inspect the malfunctioning garage door opener transmitter for a friend's mother. I used a screwdriver to open it up, and found a broken battery wire. The unit included a microcomputer and a DIP switch for a 12-bit password. I don't think I'd be revealing any great secret to tell you what her password was. It was the binary number 00000000001.

Mark Thorson (mmm@cup.portal.com)

### Ke: Airliners playing chicken (Somos and Seiler, <u>RISKS-13.82</u>)

Robert Dorsett <rdd@cactus.org> Sat, 26 Sep 92 00:50:59 CDT

Leslie J. Somos:

>I can understand preventing deployment of spoilers or thrust reversers while in >the air, but I don't understand preventing brake application.

A lot of the replies have missed a pretty fundamental component of this problem: the one of the increasing design modality of airliner systems. \*Landing\* models, \*Ground\* models, \*Takeoff\* models, \*Flight\* models, ad nauseum. Conditional logic being used to disable systems or alter the behavior of control devices to fit the projected use in a specified mode.

We have had squat switches for years. They're useful. The problem arises, as I see it, when they provide an online datum for evaluation and use by client devices in a highly abstract \*design\* context. The brake question is one such example. The brakes weren't enabled because it made no sense to enable them, from the perspective of the cockpit control logic. It's a "tidiness" that makes for clean block diagrams, but in many ways, lends a higher level of complexity to a system interface. In a conventional interface, the pilot would be able to massage the brakes to his heart's content, in the air, gear stowed, or whenever. This may not make much LOGICAL sense, though, so the feature's \*turned off\* in the air... It's yet another manifestation of the conflict of old-fashioned "open-loop" design, vs. "modern" "consider-all-cases" (and hope we got it right!) design.

### Larry Seiler:

>I agree that it is better to have an occasional accident due to a safety >interlock system that fails than to have more accidents due to people >accidentally doing fatal things like engaging the thrust reversers

I don't see this as an "override" issue. We need to differentiate between items that can cause disasters, and items that don't fit an abstract design model. A failure of thrust-reverser safety interlocks can kill an airplane, as the Lauda crash showed. "Modality" logic in the case of the brakes makes very, very little sense, however-- it's likely, as Fokker learned, that the modality \*decreased\* the safety margin, with \*no\* increase in safety in a properly-functioning system, anyway!

Technology for technology's sake, once again. Electronic toilets, anyone? :-)

[Big story on the French electronic toilets in New York in this weekend's papers! PGN]

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

### ✓ Gordon R. Dickson story "Computers Don't Argue"

Vernor Vinge <vinge%saturn@sdsu.edu> Fri, 25 Sep 92 20:23:31 -0700

The fictional story of a book club hassle escalating to a capital case
via compounded system errors:
"Computers Don't Argue" by Gordon R. Dickson, ANALOG SF&SF Magazine,
September 1965, pp.84-94.
Reprinted (as of 1976):
ANALOG 5, 1967, Doubleday, J. W. Campbell, ed.
ASTOUNDING ANALOG READER, Vol 2, 1973, Doubleday, Harrison and Aldiss, eds.
NEBULA AWARD STORIES, 1966, Doubleday, D. Knight, ed.
TRANSFORMATIONS II: UNDERSTANDING AMERICAN HISTORY THROUGH SCIENCE FICTION, 1974, Fawcett Crest Books, D. Roselle, ed.
WONDERMAKERS 2, 1972, Fantasy Premier Books, R. Hoskins, ed.

It may have been reprinted in DATAMATION, too. (But the above citations are from William G. Contento's INDEX TO SCIENCE FICTION ANTHOLOGIES AND COLLECTIONS, 1976.)

It's a great story (though by now more an archetypal contribution to RISKS than science fiction).

-- Vernor Vinge, vinge@sdsu.edu

### Re: <u>RISKS DIGEST 13.82</u>

Alex Heatley <Alex.Heatley@vuw.ac.nz> Sat, 26 Sep 92 19:22:23 +1200

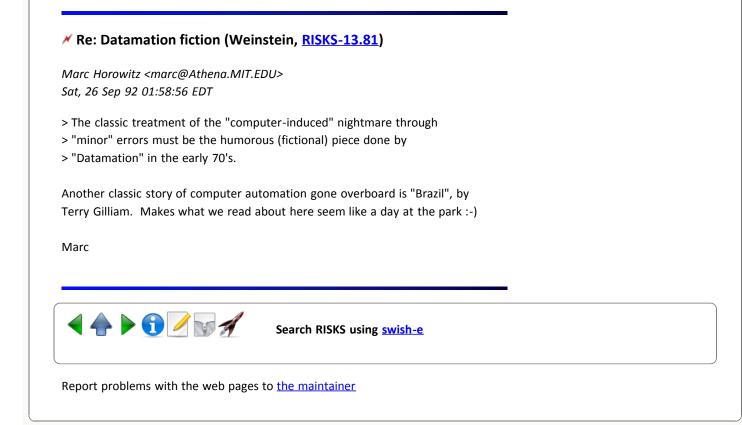
The Story of Escalating Computer Mistakes entitled "Computers Don't Argue" by Gordon R. Dickson appears in "Computer Crimes and Capers" edited by Isaac Asimov, Martin H. Greenburg and Charles G. Waugh, ISBN 0-14-007310-8 (British Edition, Published by Penguin Books), according to the title page the copyright was made by Conde Nast Publications in 1965.

This book is recommended to all risks readers for the inclusion of two stories which highlight risks related issues. The first is "An End of Spinach" by Stan Dryer (which also appeared in the Magazine of Fantasy and Science Fiction and carries a copyright of 1981) and the second is "Sam Hall" by Poul Anderson (copyright 1953 by Conde Nast Publications).

Having just flipped through the volume again I can also recommend "While-U-Wait" by Edward Wellen (copyright 1978, Magazine of Fantasy and Science Fiction).

"Computers Don't Argue" also appears in "The Best of Creative Computing Vol Two" edited by David Ahl. But it is likely that this is now out of print, however it does mention that the story originally appeared in the magazine "Analog".

It is interesting to note that many risks mentioned in this forum were considered by SF writers in the fifties and sixties...





Rebecca Mercuri <mercuri@gradient.cis.upenn.edu> Mon, 19 Oct 92 12:32:04 EDT

NCSC '92 -- Comment and Commentary Copyright (c) 1992 by Rebecca Mercuri. All Rights Reserved. Reposting and/or reprint not granted without prior written permission from the author. Address questions, response and corrections to: mercuri@gradient.cis.upenn.edu

I attended the 15th National Computer Security Conference held October 13 - 16

in balmy Baltimore MD with the hope of coming away with some solutions for the security problems I had encountered and observed over the past few years. I left with a longer list of problems, and the vague feeling that our industry has become remiss in providing us with answers that we can use, or has answers and is either incapable or unwilling to yield them publicly. Let me state clearly here that this comment does not in any way reflect negatively on the conference organizers -- they should be commended for performing their task well, creating a superbly orchestrated event which covered a broad spectrum of topics. Indeed, "rookies" were liberally mixed on panels with esteemed "greybeards" and many women (sans beards) were in evidence as session chairs and presenters (although I was somewhat dismayed to note that females appeared to constitute less than 10% of the attendees, lower than in the computing community in general). The breadth and extent of the conference does not allow one reporter to describe it fully, so I offer these remarks merely as comment and commentary, perhaps to stimulate discussion among other attendees.

The conference held an international flavor, with the keynote by Roland Hueber (Directorate General of the Commission of the European Communities) and the closing plenary on International Harmonization serving as bookends. There were repeated calls for cooperation in developing global security standards, with the primary advantages of such appearing to be in commerce. In the wake of the cold war, there seems to be a spirit of openness in this regard, but I offer the speculation that it may be foolhardy to enter into conformity of thought and solutions. Diversity, particularly in commerce, inspires creativity. Monopoly, or single-mindedness, often leaves one at risk of exploitation by a strong central power, or of attack by those who are close enough or who understand the system well enough to side-track it. We may need "faulttolerant" and "diversified" answers.

Surveying the Track Sessions:

It is useful to juxtapose thoughts about covert channels with those about encryption systems. For the uninitiated, covert channels (to a first approximation on a definition) are created when internal intermittent polling is performed in an effort to conceal illicit data collection activities. Bob Morris provided the statistic that 1/10 of a bit per second is enough to expose a key in approximately 1 month. This is at current processing rates, but one can extrapolate out the Silicon Valley curve and surmise that our current key encryption systems will be inadequate within the end of the century (if not now, perhaps).

In the quest for tools one encounters the debate on provability and formal top level specification. Virgil Gligor referred to "formal top level specification as an unmitigated waste of time," saying that data structures and source may not map to the top level, there may not be enough relevant details provided, and excessive false illegal flows may occur. Earl Boebert stated that formal proving methods have worth in analysis of specifications, but have failed utterly in spec/code, code/object, and code/behavior correspondence. Still, formal methods have their supporters, most notably SRI, as indicated by John Rushby, one of their directors (who also publicly revealed that there had been a major successful break-in at the lab last month). Interestingly, the panel on Intrusion Detection was chaired by SRI's Teresa Lunt, who discussed the use of expert systems to encode vulnerabilities, attack methods and known suspicious behaviors. Steve Snapp expressed the divide and conquer approach, saying that there may be no single generalizable model of intrusion, and that static, incidence/existence, and data driven methods should all be used.

The matter of viruses was explored throughout various sessions. The general consensus of opinion seemed to be that rigorous procedures and policies need to be implemented so that recovery is possible to some level following contamination or invasion. In the talks I attended, no clear method for handling the recovery from a "new" virus (that can not be eradicated with existing software) was offered. This was not consoling to someone who had just last week left a client's law office with the admonishment "don't use any of the text files that you've created in the last 6 months until I can find out what the new virus strain is that appears to have adhered to some unknown quantity of them." Here too, the standardization on certain operating systems and environments (such as Microsoft Windows(TM)), and uniform acceptance of specific tools (such as the legal community's reliance on Word Perfect(TM)) encourages the proliferation of attacks that could potentially disable large sectors of the user base.

Losses seem to be tied heavily to the bottom line. In banking, it may not be advantageous to implement a \$10M or more security system that still does not assure total impenetrability when insurance coverage can be obtained at a cost of \$1M (even if this price only remains low until there is a hit). In health care, as described in Deborah Hamilton's award- winning paper, the bottom line may indeed be one or more people's lives. As true with drug approvals, it is easy to see that holding back an inadequately tested computer system may cost more lives than providing it while continuing to make improvements and corrections. How does one weigh security, reliability and verifiability issues when there is a crying need for access to the developing technology? We are faced with a moral dilemma without a governing body to set policies.

The area of privacy was eloquently addressed by Attorney Christine Axsmith who said that our reasonable expectations of privacy, as expressed by the 4th Amendment, protect people, not just places. But she went on to say that with regard to the computer industry, the Privacy Act and other legislation efforts still suffer from a lack of court rulings necessary to define their interpretations. Will our efforts to improve security undermine privacy? Curt Symes (from IBM) stated that "we'll all be using smart cards in the future, for a higher level of authentication." Does this mean that I will eventually be required to be bioidentified (DNA, fingerprint, retinal scan, voiceprint) in order to obtain access to my own data and research? A chilling thought.

In conclusion, to paraphrase Peter Neumann (which seems only fitting, as he "scooped" my Nov. 92 CACM Inside Risks column on voting machines by referring to some of its salient points in his banquet address, without citation) -perhaps the conference theme "Information Systems Security: Building Blocks to the Future" should be read not as "building-blocks" (the small bricks), but as "building BLOCKS" or obstacles to our future as security professionals. There is a sense of urgency now -- many of us need more than a foundation of toy blocks, requiring true solutions which appear to not be forthcoming. What we don't want are systems and design structures that are so cumbersome as to impede computational progress. Discussion may be fruitful, but let us all get our noses to the grindstone and provide functional tools and answers, rather than guidelines and assertions. Some are working in this direction, others are needed.

### Vote Early, Vote Often

Bear Giles <bear@tigger.cs.colorado.edu> Thu, 8 Oct 1992 10:35:12 -0600

A local proponent of voting-by-phone keeps pointing to the 'safety' of absentee ballots as evidence that phone-voting would be safe. So it was with more than passing interest that I read the lead article in the \_Rocky Mountain News\_ today....

(Main headline [1]) Vote fraud riddles Colorado County

'Vote early, vote often' was Costilla County pattern, judge rules. Non-residents used absentee ballots to help pals win office

(Article headline)

Judge finds Costilla County riddled with election fraud

Non-residents marked absentee ballots to help friends, relatives wind elections, court rules

by Dick Foster Rocky Mountain News Southern Bureau

Widespread election fraud has been uncovered in Costilla County [in south-central Colorado abutting New Mexico], where evidence shows people cast absentee ballots for friends and relatives seeking public office back to 1984.

One of those who cast an absentee ballot in the southern Colorado county was not even a U.S. citizen. Another was an imprisoned felon, evidence shows.

Another 106 people who had cast ballots in one or more of the last four elections lived nowhere near Costilla County and had no claim to an absentee vote, Chief District Judge Robert Ogburn of Monte Vista ruled.

It took the action of citizens banding together to file a civil lawsuit to halt the abuses after their complaints were rebuffed by the Colorado secretary of state's office and the local district attorney.

Office holders felt "entitled" to collect as many absentee votes as possible from children who had long ago left the county "as well as from nieces and nephews and anyone else who bore the slightest resemblance to being a relative," said Ogburn. "Over the years, the practice expanded to include friends who had left the community to live elsewhere."

One Mexican national with a green card testified that a county commissioner solicited his vote and gave him an absentee ballot.

Many of the absentee voters gave fake addresses in the county. Others simply used local post office box numbers as their claim to local residence.

Ogburn called one box "famous" -- it had been claimed by several absentee voters.

Costilla County had 254 absentee ballots in the 1990 general election, about 14% of the county's total vote of 1,827. In neighboring counties, only 5% to 7% of the votes were absentee.

At least once, absentee ballots meant the difference between victory and defeat for incumbents. In 1988, a resident named Lillian Maestas ran against county clerk and recorder Roy D. Martinez. She led in election day returns, but lost when the absentee votes were counted, said Wilmer Pacheco, a Maestas campaign worker.

"Some of these people haven't lived here since World War II and they're voting here. When you have that many votes in a small county it's going to throw the election," said Stephanie Kimbrel, one resident who helped organize Citizens for Better Government after the August primary election. The group launched its own investigation and civil lawsuit to stop voting abuse.

Urcilia Auth joined the group after returning to San Luis to retire and serving as a poll watcher during the August primary. "I saw people I knew from Alamosa [in a different county] come in here and cast ballots," she said. "But the county clerk hadn't given us a challenge list so we couldn't challenge them. And names appeared on the registration list of some people I know who live in Colorado Springs."

The residents said they grew angrier when their calls for an investigation of election abuse where turned aside by the secretary of state's office and Alamosa County District Attorney Douglas Primavera.

"When I took this to Donetta Davidson, the elections director at the secretary of state's office, after the August primary, she told me that we should hire a lawyer because their office has no responsibility at all in these matters," said Kimbrel.

Secretary of State Natalie Meyer told the \_Rocky Mountain News\_ Wednesday "the law does not give me any authority to do anything" to investigate election abuses. Such matters are for the district attorney to investigate, she said.

Primavera told the \_Rocky Mountain News\_ his office lacked the staff to conduct an investigation into the residents' allegations.

"They all just passed the buck," Pacheco said.

The residents hired Alamosa attorney Martin Gonzales, who filed a civil lawsuit in September challenging 108 names of absentee voters in the county. The residents themselves gathered records and witnesses to prove the voters were not county residents.

"I think the secretary of state's office could have stepped in," Gonzales said. "They didn't." [1] The \_Rocky\_ is printed in tabloid format, not broadsheet. The front page is a collection of headlines and a large photo; the lead story can appear anywhere in the paper. The \_Rocky\_ is \_not\_ a tabloid paper in the style of the Weekly World News\_ --- it is one of two leading newspapers in Colorado and choose the tabloid format for marketing reasons around 50 years ago.

Bear Giles bear@fsl.noaa.gov

### \* Toronto Teenager Charged in 911 Case

Nigel Allen <Nigel.Allen@lambada.oit.unc.edu> Wed, 7 Oct 1992 21:51:00 GMT

Here is a press release that I received from the Metropolitan Toronto Police. The Toronto Star ran a story (based on the press release) on its front page today (October 7).

1992 October 06, 1950 hours

Teenage Computer Hacker Nabbed by Police

Detectives from the Major Crime Squad at Police Headquarters have arrested a 15-year-old North York boy and charged him with a number of computer-related crimes. Investigations have revealed that on some occasions his pranks paralyzed the Metropolitan Toronto 911 emergency telephone system.

Last July, a young man called the 911 emergency number from a location in the west end of Metropolitan Toronto and reported a number of medical emergencies which caused units from the Metropolitan Toronto Police, ambulance services and local fire departments to respond. All of these calls were determined to be false.

On one occasion, he totally monopolized the 911 system and rendered it inoperable thereby denying citizens access to the 911 lifeline throughout the Metropolitan Toronto area.

Bell Canada security officers assisted police in their search for the source of the calls. Acting on a Criminal Code search warrant, police today entered a North York home, seized a quantity of computers and arrested a teen-age boy. He is to appear in Youth Court, 47 Sheppard Avenue East, North York, Friday, November 6, 1992, charged with theft of telecommunications, 24 counts of mischief and 10 counts of convey false message.

Investigations are continuing.

(end of press release)

Note from NDA: More information may be available from the public affairs office of the Metropolitan Toronto Police at (416) 324-2222 or from Detective W. Johnston of the Major Crime Squad at (416) 324-6245.

[The usual disclaimers: No connection with any police agency, telephone company or obnoxious teenagers who think false alarms are amusing. The opinions expressed are not necessarily those of the University of North Carolina at Chapel Hill, the Campus Office for Information Technology, or the Experimental Bulletin Board Service. internet: bbs.oit.unc.edu or 152.2.22.80]

### Matter students charged with scholarship scam

"Peter G. Neumann" <neumann@csl.sri.com> Sun, 11 Oct 92 15:45:15 PDT

NEW BRUNSWICK, N.J. (UPI) -- Three Rutgers University students have been charged with trying to bilk their fellow students with a fake scholarship scam. The trio allegedly placed fliers around campus advertising ``New Jersey Scholarship and Grant Search Services,'' directing applicants to send Social Security and bank account numbers and credit card data to a mailing address. Police say they used the information to apply for duplicate birth certificates.

Police say they have located only one victim who actually lost money, a Livingston College student who had \$1,000 withdrawn from her bank account. But another women allegedly reported that she had received notices from credit card companies that someone was trying to obtain cards using her name.

Police have charged Justin Okieze, 18, of North Brunswick; Robert Harrell, 21, of New Brunswick; and Lisa Young, 20, of Edison, with theft by deception.

### A320 engine control problem at Gatwick

John Rushby <RUSHBY@csl.sri.com> Sat 10 Oct 92 10:41:43-PDT

Source: dp:DPA:Deutsche Press-Agentur

LONDON (OCT. 8) DPA - A fully-laden Airbus A 320 lost power in one engine for no accountable reason while approaching London's Gatwick airport, necessitating emergency procedures, it was reported Thursday.

This suggested that computers controlling the engine 'could be capable of developing a mind of their own and countermanding decisions made by the crew', The Times newspaper said.

The aircraft of the Air 2000 charter company was on its way from Venice to Gatwick with 135 Passengers and seven crew September 26 when the starboard engine continued to 'wind down' until well below the required flight idle speed, the newspaper said.

The captain had to shut the engine down completely - a routine operation that did not affect safety - and then restarted the engine at 14,000 feet to make a normal two-engined landing.

'Despite a detailed check of all the systems, the fault has not been traced, but it is believed to involve the engine overspeed valve which restricts the flow of fuel to the engine as power is cut,' the newspaper said.

## 🗡 T\* S\*

<Anonymous Bosh> Mon, 12 Oct 92 6:33:26 PDT

Today in a meeting, it was brought up that some one had emailed a message and most likely added the words T\*\* Sec\*\*t in jest or fun. The message body was apparently one of those systems which can include the bitmap for a military service which will remain nameless. Some how or other the DoD got this message and started an investigation. Needless to say, the DoD was not amused, this despite system wide disclaimers that said systems are not to be used for classified work. Ah! The electronic future is going to be an interesting one.

### Model DEA mishandling of national security information

"Philip R. Moyer" <prm@ecn.purdue.edu> Mon, 12 Oct 92 14:23:47 -0500

This is a brief overview of a General Accounting Office (GAO) review of computer security procedures at the Drug Enforcement Administration (DEA).

The results of the GAO investigation showed that DEA is not adequately protecting national security information in its computer systems, and that though the DEA knows of no unauthorized disclosures, revelations of this national security information would endanger lives and hinder US drug enforcement and interdiction programs.

The Department of Justice requires that all of its component agencies identify all computers used to process national security information. DEA, however, has failed to do so. DEA's report was produced by the Office of Security Programs based on a survey. Ommisions in DEAs report were caused because the headquarters was not surveyed, and because one field division did not respond to the request for information. Another field division reported that they did not have any computers processing national security information when in fact, the GAO found that they do.

DEA was in violation of National Security Guidelines by

- using the office automation system to process classified data. This system has not been approved or safeguarded for processing classified data.
- not conducting a risk analysis of the system.
- operating said office automation workstations in open, unshielded work areas.
- using non-TEMPEST rated workstations to process national security information.
- using unencrypted data communications lines.

Additional problems occur because DEA uses the Office Automation system to process national security information. For example, any DEA employee, regardless of clearance, has access to any information stored in any of the office automation workstations. Also, vendor-issued system passwords have not been changed, so the vendor and other knowledgable individuals would have complete access to the system (which was installed in 1987).

Some DEA personnel were processing classified information on microcomputers that had fixed hard disks, which, in some cases, results in the inadvertant storage of classified information on that disk, where it can later be revealed to individuals without clearance (see GAO/T-IMTEC-91-6 for examples).

In addition to the information security problems outlined above, DEA has the following physical security problems, which increase the risk from the above problems:

- inadequately controlled access to sensitive areas
- individuals without national security clearances working unescorted in sensitive areas
- unattended computers left logged on
- computer-generated printouts and disks being left unattended and unsecured
- documents left unattended and unsecured
- safes left open and unattended

A specific example mentioned was that janitors are left unattended in areas where computers were used to process national security information, and that those computers were left logged on at the time. These janitors had neither a clearance nor a need to know.

Non-computer related physical security problems include

- electronic card key devices are disabled during working hours and doors are propped open
- security staff fail to review card-key logs
- stolen or lost keycards are not deactivated
- non-DEA employes have key cards that open sensitive areas within DEA
- locks on division offices have not been changed since 1985, even though 17 keys have been lost or stolen, including masters to computer areas
- DEA employees are not required to wear identification badges

The report concludes that these security weaknesses endanger the lives of federal agents and need to be corrected immediately.

The document summarized in this article is GAO/IMTEC-92-31. The GAO makes one copy of each report available for free; additional copies are \$2.00. Orders can be sent to

U.S. General Accounting Office P.O. Box 6015 Gaithersburg, MD 20877 or phone them in at 202-275-6241. Phil

### ✓ Using the DOT's computers to steal car stereos

Bill Marshall <marshall@cs.iastate.edu> Wed, 14 Oct 1992 00:25:13 GMT

>From the Des Moines (Iowa) Register, Friday, October 9, 1992, page 1M

Car break-in ring cracked; youth shows the way

By Tom Alex - Register Staff Writer

[I have only entered the paragraphs that containted computer information]

Des Moines police this week broke a sophisticated youth theft ring that was using license plate numbers and state records to locate cars for late-night break-ins.

The youths would spot cars with expensive stereo gear in parking lots during the day and then use Iowa Department of Transportation computer records to determine where cars would be parked at night.

With the license plate numbers, the teen-ager went to an Iowa Department of Transportation office at Park Fair Mall and used public access computers to learn the home addresses of the owners of the vehicles.

He and his cohorts didn't want to break into the vehicles when there were a lot of potential witnesses around, police said, so they found addresses from registration information and visited the victims at their leisure.

Security problems with public access computers cropped up last year shortly after the computer terminals were installed, said Jan Hardy, assistant office director with vehicle registration.

A case worked in the juvenile system reported having a client who had been using the terminals for illegal activities.

Sortly afterward, officials developed a security system to help curtail illegal acts. People wishing to look up license plate numbers must identify themselves to the computer.

"If they use the front counter terminal and sign on themselves, that does provide at least some tracking of inquires," said Hardy.

marshall@cs.iastate.edu Bill Marshall, Computer Science Department, Iowa State University

### Robot daydreaming

Les Earnest <les@sail.stanford.edu> Sat, 10 Oct 92 11:39:50 -0700

Copyright 1992 by UPI. Reposted with permission from the ClariNet

Electronic Newspaper newsgroup clari.news.interest.quirks. For more info on ClariNet, write to info@clarinet.com or phone 1-800-USE-NETS.

STANFORD, Calif. (UPI) -- Stanford University Hospital removed its new robotic transportation devices from service Thursday after one of the units went awry and fell down a set of stairs.

Associate hospital director Louis Saksen said no one was injured when the robot veered off course and tumbled down the steps.

Stanford purchased three of the units to perform simple tasks, such as delivering food trays to patients and transporting X-rays and supplies around the hosptial.

The facility has been phasing in the units for use this fall and has had no problems with the robots during their first weeks of the trial period.

Officials said they had no idea what caused the robot to malfunction when it returned from delivering a food tray to a patient.

Saksen said the robots are designed to free hosptial workers from routine duties to do other, more vital work.

The battery-operated devices have been used for similar duties in several hospitals across the United States.

[David Cheriton remarks that it was probably garbage collecting at the time. That's the logical thing to do after delivering food. -Les Earnest (les@cs.stanford.edu)]

# Announcement (fwd)

"Lance J. Hoffman" <hoffman@seas.gwu.edu> Wed, 14 Oct 92 11:38:51 EDT

[From Professor Lance J. Hoffman, Department of Electrical Engineering and Computer Science The George Washington University Washington, D. C. 20052 (202) 994-4955 fax: (202) 994-0227 hoffman@seas.gwu.edu]

Forwarded message: Date: Wed, 14 Oct 92 09:10:37 -0400 From: rweingar@cs.UMD.EDU (Rick Weingarten) Subject: Announcement

The Computing Research Association (CRA), a nonprofit association in Washington, DC, seeks a motivated staff policy associate with a computer science or engineering background and an interest in public policy. In conjunction with the Association for Computing Machinery (ACM), CRA will be significantly expanding its coverage of public policy issues affecting the computing community. This entry-level position offers an exciting opportunity to be involved in policy-making, as it relates to computers and information technology. Issues CRA currently is following include:

\* Long-term changes in the way government supports R&D;

\* The High-Performance Computing and Communications initiative, including the National Research and Education Network (NREN);

\* Digital libraries; and

\* Information policies, including privacy, security, intellectual property and public access to government information.

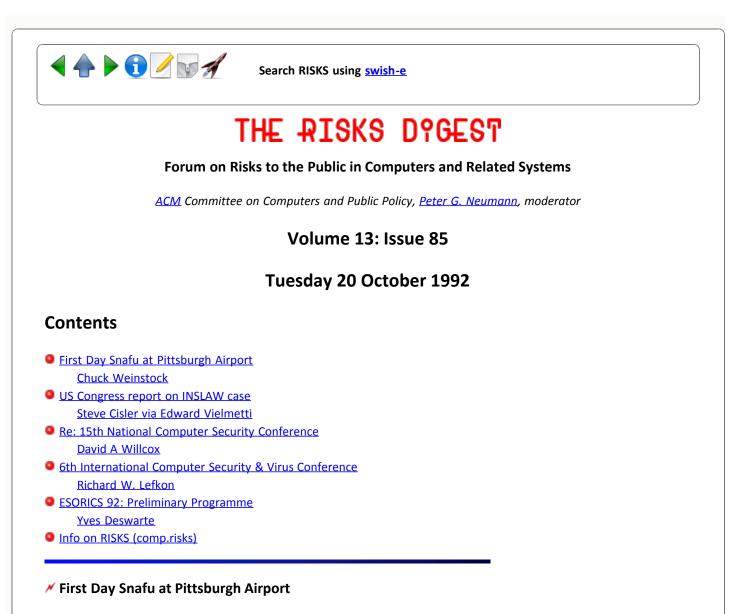
The associate will track the development of issues, perform research, attend meetings and communicate with experts in the field. Through written and oral communications, the policy associate and the executive director will inform the computing community about important issues. The associate will work with CRA and ACM committees to set priorities and strategies for further action, such as drafting letters and testimony, convening workshops and seminars, and developing position papers. In addition to a computer science or engineering background, the associate must have excellent communication skills. Knowledge of the legislative process and public policy experience are a plus. A bachelor's degree is required. The salary for this entry-level position is commensurate with that of similar policy jobs in the Washington area. CRA offers a good benefits package. Send cover letter, salary requirements, resume and three appropriate writing samples to

Fred W. Weingarten, Executive Director Computing Research Association 1875 Connecticut Ave. NW, Suite 718 Washington, DC 20009.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Chuck Weinstock <weinstoc@SEI.CMU.EDU> Mon, 05 Oct 92 12:12:49 EDT

I left Pittsburgh for a meeting in Chicago on Wednesday, September 30th. I returned on Friday, October 2nd. In between the old Pittsburgh airport closed and the new one began to operate. According to a friend who changed planes in Pittsburgh on opening day (Thursday), things went smoothly. That may have been true for folks hubbing at the airport, but for those Pittsburgh bound it apparently was not.

In order to more easily retrieve my car I had parked with one of the off-airport parking services. Upon return I asked the van driver how things had gone the day before. He said that everything had gone pretty smoothly, except for baggage claiming. He said that delays were around 40 minutes in the morning, but had stretched to two hours by the afternoon. The supposed reason: the airport has a new automated baggage handling system that reads bar codes off luggage. A Britsh Air 747 had arrived with uncoded luggage, and the machinery didn't know how to cope.

**Chuck Weinstock** 

### ✓ US Congress report on INSLAW case

Edward Vielmetti <emv@msen.com> Sat, 10 Oct 92 16:05:48 EDT

To: comp-archives@ucbvax.Berkeley.EDU From: sac@Apple.COM (Steve Cisler) Newsgroups: comp.archives Subject: U.S. Congress Report on Inslaw case Keywords: Inslaw, Promis, Dept. of Justice Date: 10 Oct 92 19:20:50 GMT

OCR version of The U.S. Congress House report, "The Inslaw Affair". Rendered into electronic file by <pinknoiz@well.sf.ca.us>

Available on ftp.apple.com in the ftp/alug/rights directory 421 kb.

### Ke: 15th National Computer Security Conference (Mercuri, <u>RISKS-13.85</u>)

David A Willcox <willcox@urbana.mcd.mot.com> Tue, 20 Oct 1992 15:36:36 GMT

>In the quest for tools one encounters the debate on provability and formal top >level specification. Virgil Gligor referred to "formal top level specification >as an unmitigated waste of time," saying that data structures and source may >not map to the top level, there may not be enough relevant details provided, >and excessive false illegal flows may occur. ...

A point of clarification: He didn't say that formal top level specifications were a waste of time, but that doing covert channel analysis on them was an \_unmitigated\_ (his emphasis) waste of time. His point was that you had to do a CC analysis on the source code anyway (since channels would appear in code that didn't show up in the specs). Since any channel found in the analysis of the spec would also be found in the analysis of the code, and you have to do the latter, anyway, doing the former is not useful. (This, of course, flies in the face of the principle that it's much cheaper to find a bug found early in the development process than late, but that's another discussion. Perhaps doing the covert channel analysis is more expensive than fixing a specification bug when you are done with the code.)

### On another topic...

I think that the most surprising new proposal came in the session on the FBI's Digital Telephony Initiative. (This is the proposed legislation that would require telephone and data transport providers to build wiretap capabilities into their systemms.) Someone pointed out that the really bad guys would just use encryption for their data transmission, and that wiretapping wouldn't gain any information on them. (The FBI doesn't want to deal with encryption right now. They'll think about that when (if) they get the current proposal passed.) Dorothy Denning suggested that anyone using high-level encryption over a public network be required to register their encryption keys with some agency. This agency would then distribute the keys when an appropriate court order was presented. The risks of this are fairly obvious.

David A. Willcox, Motorola MCG - Urbana, 1101 E. University Ave., Urbana, IL 61801 217-384-8534 ...!uiucuxc!udc!willcox willcox@urbana.mcd.mot.com

### 6th International Computer Security & Virus Conference

Richard W. Lefkon <dklefkon@well.sf.ca.us> Sat, 3 Oct 1992 09:31:35 -0700

CONFERENCE ANNOUNCEMENT: 6TH INTERNATIONAL COMPUTER SECURITY & VIRUS (no charge for exhibits only - complete & fax form by 11/27) Wednesday Thru Friday March 10-12, 1993, New York Ramada

spons by DPMA Fin.Ind.Ch. in coop with ACM-SIGSAC, IEEE Computer Society, Boston Comp Soc, Comms Mgrs Assn, Corp for Open Systems, EDP Aud Assn (Ph), Info Sys Sec Assn (NY), NetWare Users Intl (NYLA)

- \* 5 tracks, 53 Vendors, 90 Speakers (first 24 speakers & chairs below)
- \* Identify Latest Threats to SNA, DEC, PC, MAC, X.25, OS2, ISDN, UNIXX
- \* Tools & Techniques: Learn What Major Corp's & Agencies Are Doing
- \* Specific Countermeasures: From Labs, Other Co's, Commercial Vendors
- \* Network One-to-One with the Experts & Your Counterparts Elsewhere
- \* 870-page 1993 bound Proceedings containing all papers
- \* Breakfast & Beverage breaks, Luncheon, Empire State Building Reception
- \* Entire Large Floor, Across from Penn Station & Garden, Parking Avail
- \* Group Prepayment Discount: \$975 total for FOUR (4) CONF REGISTRATIONS

PRELIMINARY PROGRAM: 3 TRACKS BELOW, PLUS ONE EACH PC/LAN & MF/COM PRODS.

CIO/SVP Management/Practice Technical & Research Full-Day LAN/LAW

3/10 Wed am courses: Intro Computer Security & Viruses NetWare Setups 1:00 courses: Telecom Managemt Virus Tech Intro: Skulason Vines Setups dinner: "Why Don't They Nail/Jail 'Em All?" vs. "Viruses as Free Speech"

3/11 Thursday:
9:00 Keynote Address: Seamless Security
10:15 Telecom I: Toll Fraud IBM Security Approach LAN HW/SW Defenses
R.Lefkon, NYU W.Vance, IBM (spkr) P.Peterson, MrtnM
12:00 (Buffet & Restaurant Luncheon Provided)
1:00 Risk Assessmt Panel MAC Attacks I Disinfecting Server
Katzke/Gilbert, NIST J.Paradise, Apple H.Highland,Compulit
2:30 Encryption, RSA, etc. UNIX Security I LAN Policy & Disaster
W.Murray, Deloitte T.Duff, Bell Labs K.van Wyk, CERT/CMU
4:00 TransBorders: EC,Law What's Wrong With AntiVirus Products & Testing
E.Okamoto, MITI G.Drusdow, F.Skulason, A.Solomon, P.Tippett, etc.
6:00 Empire State Building Observatory "MEET THE EXPERTS" Sit-Down Reception

3/12 Friday:

9:00	Publicly Avail	Help Te	kkies' Delight	Intrusion	DetectPrev		
	K.Brunnstein,U.	Hamburg	F.Cohen, ASP	D.Park	er, SRI		
11:00	MAC II & DEC	Attacks	UNIX Security	II Using	CCrime Law	, FBI	
	E.Spafford,(s)Pu	irdue K.I	_evitt, U.C.Davis	s J.Bloomb	ecker (s)		
	"ET TU HACKE					heated view	s,
	incl R.Schiffreer						
3:15	WAN/Warfare	/Telecom	II New Researc	ch & Ideas	Recent CCr	ime Cases	
	G.Mallen, Mexi		kulason, F-Prot				
4:45			ecurity Product				
			,				
ххх	xxxxxxxxxxxx	xxxxxxx	xxxxxxxxxxxx	xxxxxxxx	хххххххх	ххххххххх	xxxx
Х			Х				
Х	SIXTH INTERNA	TIONAL CO	OMPUTER SECU	IRITY & VIRI	JS CONFERI	ENCE X	
Х	Wednesday tl	nru Friday	March 10-12,	1993, NY Ra	imada 🔰	X	
Х			Х				
Х	Application for	free pass	to exhibits (late	e price: \$30.	00) X		
Х	Fax to (303) 825-9151 by November 27, 1992 X						
Х	or postma	rk to Box	894 New York	NY 10268	Х		
Х			х				
X Fi	rst Name:		La	ist:		X	
Х			х				
хо	rganization:			Title:		Χ	
Х			х				
X St	treet Address: _					X	
Х			х				
X Ci	ity:		State/Prov	/: Pos	stCode:	X	
х			х				
X D	ay Telephone:	()	Fax	Telphone:		_ X	
х			x				
хс	OPTIONAL: [_] C	HECK IF II	NTERESTED IN (	CONF SESSIO	ONS & COU	RSES X	
ххх	xxxxxxxxxxxx	xxxxxxx	****	xxxxxxxx	xxxxxxxx	ххххххххх	xxxx

# ✓ ESORICS 92: Preliminary Programme

Yves Deswarte <deswarte@laas.laas.fr> Wed, 14 Oct 1992 16:47:35 +0100

===== Yves Deswarte - LAAS-CNRS & INRIA - 31077 Toulouse (France) ===== ==== E-mail:deswarte@laas.fr - Tel:+33/61336288 - Fax:+33/61336411 ====

#### ESORICS 92

**Final Programme** 

European Symposium on Research in Computer Security November 23-25, 1992, Toulouse, France

Computer security is concerned with the protection of information in environments where there is a possibility of intrusion or malicious action. The aim of ESORICS 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 under the best conditions, ESORICS 92 will be a single track symposium and the selected papers will be presented in a conference hall whose capacity is 290 attendees. ESORICS 92 is the second symposium of a series started with ESORICS 90 held in Toulouse in October, 1990.

Symposium Chair: Gerard Eizenberg (ONERA/CERT, France)

Organized by AFCET

In Cooperation with

BCS The British Computer Society

CNRS Centre National de la Recherche Scientifique

DISSI Delegation Interministerielle pour la Securite des Systemes d'Information

DRET Direction des Recherches Etudes et Techniques

ERCIM European Research Consortium for Informatics and Mathematics

GI Gesellschaft fur Informatik

IEE The Institution of Electrical Engineers

INRIA Institut National de Recherche en Informatique et Automatique

NGI Nederlands Genootschap voor Informatica

### PROGRAMME

Monday, November 23, 1992

9:00-10:30 Registration and welcome coffee

10:30-11:00 Introduction to ESORICS 92

11:00-12:30 Session: Access Control (Chair: Jeremy Jacob)

Towards security in an open systems federation (John A. Bull, Li Gong, Karen R. Sollins)

Type-level access controls for distributed structurally object-oriented database systems (Udo Kelter)

On the Chinese wall model (Volker Kessler)

12:30-14:15 Lunch

14:15-15:45 Session: Formal Methods (Chair: Brian Randell)

Formal methods and automated tool for timing-channel identification in TCB source code (Jingsha He, Virgil D. Gligor)

Separating the specification and implementation phases in cryptography (Marie-Jeanne Toussaint)

Formal specification of security requirements using the theory of

normative positions (Andrew J. I. Jones, Marek Sergot)

15:45-16:15 Break

16:15-17:45 Invited Talks

Roger Needham: Key management

Yvo Desmedt: Breaking the Traditional Computer Security Barriers

18:00-... Buffet

18:30-... Poster Session

Posters:

Schema de protection et systemes d'information (Patrick Trane, Jean-Marie Place) ASAX: Universal Tool for Audit Trail Analysis (B. Le Charlier et al.) Verification of Security Protocols (J.-R. Abrial, P. Bieber, E. van Wickeren) Bases de donnees reparties et securite (S. Moalla) RACE/Securenet Project (D. Karagiannis et al.) An Approach to the Evaluation of Operational Security of Computing Systems (M. Dacier, M. Kaaniche) Software with integrity - the key to secure applications (A. Wood, N. Poulter) Smart Cards and Public Key to Accreditations Management (Didier Angebaud, Pierre Paradinas) R&D Items on Distributed Systems Security (Manel Medina) L'enseignement de la securite informatique en France (Michel Dupuy) Tuesday, November 24, 1992 8:30-9:00 Welcome coffee 9:00-10:30 Session: Authentication I (Chair: Thomas Beth) Verification and modelling of authentication protocols (Ralf C. Hauser, E. Stewart Lee) KryptoKnight authentication and key distribution system (Refik Molva, Gene Tsudik, Els Van Herreweghen, Stefano Zatti) Associating metrics to certification paths (Anas Tarah, Christian Huitema) 10:30-11:00 Break 11:00-12:30 Session: Distributed Systems (Chair: Catherine Meadows) An object-oriented view of fragmented data processing for fault and intrusion tolerance in distributed systems (Jean-Charles Fabre, Brian Randell) The development and testing of the identity-based conference key distribution system for the RHODOS distributed system (Michael Wang, Andrzej Goscinski) Policy enforcement in stub autonomous domains (Gene Tsudik) 12:30-14:15 Lunch 14:15-15:45 Session: Authentication II Freshness assurance of authentication protocols (Kwok-Yan Lam, Dieter Gollmann) A formal framework for authentication (Colin Boyd) Timely authentication in distributed systems (Kwok-Yan Lam, Thomas Beth) 15:45-16:15 Break 16:15-17:00 Invited Talk Yvon Klein: What research for security evaluation ? 17:00-18:15 Panel: Availability and Integrity Chair: Gerard Eizenberg, Participants: Thomas Beth, Frederic Cuppens, Sushil Jajodia, Jean-Claude Laprie 18:30-... Poster Session 20:00-... Banquet Wednesday, November 25, 1992 8:30-9:00 Welcome coffee 9:00-10:30 Session: Database Security (Chair: Robert Demolombe)

Polyinstantiation for cover stories (Ravi S. Sandhu, Sushil Jajodia) On transaction processing for multilevel secure replicated databases (Iwen E. Kang, Thomas F. Keefe) Security constraint processing in multilevel secure AMAC schemata (Gunther Pernul) 10:30-11:00 Break 11:00-12:00 Session: System Architectures M2S: A machine for multilevel security (Bruno d'Ausbourg, Jean-Henri Llareus) GDoM, a multilevel document manager (Christel Calas) 12:00-13:45 Lunch 13:45-15:15 Session: Applications (Chair: Michel Dupuy) UEPS - A second generation electronic wallet (Ross J. Anderson) A hardware design model for cryptographic algorithms (Joan Daemen, Rene Govaerts, Joos Vandewalle) ASAX: Software architecture and rule-based language for universal audit trail analysis (Naji Habra, B. Le Charlier, A. Mounji, I. Mathieu) 15:15-15:30 Closing Remarks Programme Committee: Jean-Jacques Quisquater (UCL, Belgium), Chair Bruno d'Ausbourg (ONERA-CERT, France) Joachim Biskup (Universitat Hildesheim, Germany) Peter Bottomley (RSRE, United Kingdom) Yvo Desmedt (University of Wisconsin-Milwaukee, USA) Yves Deswarte (LAAS-CNRS & INRIA, France) Gerard Eizenberg (ONERA-CERT, France) Amos Fiat (University of Tel-Aviv, Israel) Dieter Gollmann (University of London, United Kingdom) Franz-Peter Heider (GEI, Germany) Jeremy Jacob (Oxford University, United Kingdom) Helmut Kurth (IABG, Germany) Jean-Claude Laprie (LAAS-CNRS, France) Peter Landrock (Aarhus University, Denmark) Teresa Lunt (SRI International, USA) John McDermid (University of York, United Kingdom) John McLean (NRL, USA) Catherine Meadows (NRL, USA) Jonathan Millen (MITRE, USA) Emilio Montolivo (Fondazione Ugo Bordoni, Italy) Roger Needham (University of Cambridge, United Kingdom) Alfredo de Santis (Universita di Salerno, Italy) Einar Snekkenes (NDRE, Norway) Marie-Jeanne Toussaint (Universite de Liege, Belgium) Kioumars Yazdanian (ONERA-CERT, France) Organization Committee: Yves Deswarte (LAAS-CNRS & INRIA, France), Chair Laurent Cabirol (SCSSI, France) Jean-Francois Cornet (Consultant, France) Michel Dupuy (ENST, France) Marie-Therese Ippolito (LAAS-CNRS, France) Marie-France Kalogera (AFCET, France)

Paul Richy (CNET, France)

Pierre Rolin (ENSTA, France) Kioumars Yazdanian (ONERA-CERT, France)

#### **GENERAL INFORMATION:**

Symposium Location: Hotel Palladia

271 avenue de Grande Bretagne, 31300 Toulouse, France telephone: +33 62 120 120, fax: +33 62 120 121 Hotel Palladia is located in the west district of Toulouse, 5 km from city centre.

Access to Toulouse:

- By plane: Toulouse-Blagnac International Airport (telephone: +33 61 42 44 00). Hotel Palladia is 4 km from the airport. Approximate taxi fare is 50 FF.
- By train: Toulouse-Matabiau railway station (telephone:
  +33 61 62 50 50). Bus 14 from railway station to "Chardonnet" stop (in front of Hotel Palladia). Approximate taxi fare is 70FF.
- By car: Toulouse is linked to the main European road networks.
   On the Toulouse ring, direction Auch, exit 1 to Casselardit-Purpan.

Tourist Information: Office du Tourisme, Donjon du Capitole, 31000 Toulouse, telephone: +33 61 11 02 22

Visa: For non European Community citizens, please check with the French Consulate in your home country if you need a visa. Visa applications take approximately 4 weeks to process.

**Registration Procedure:** 

- Advance: Please complete the registration form and send it to AFCET. About 15 days before the beginning of the symposium, registered participants will receive their pass, which is to be presented at the registration desk to receive symposium documents.
- On-Site: Registration desk and welcome service will be available from 8:30 am to 8:00 pm on Monday 23, to 7:30 pm on Tuesday 24 and to 4:00 pm on Wednesday 25.
- Fellowships: Applications for half-rate registrations can be sent to AFCET with due justification. Students wishing to apply for these fellowships should join a recommendation letter from their professor.
- Fees: Registrations fees include admission to the technical sessions, one copy of the proceedings, breaks, lunches, Monday buffet and Tuesday banquet.

Payments: Payments are accepted in French Francs only:

- by credit cards (Visa International or MasterCard only): complete the charge authorization on the registration form.
- by banker's draft (with indication of your name and ESORICS 92), to the order of AFCET, bank account 502 650 009-02 at BIMP, 22 rue Pasquier, 75008 Paris, France. Please ask your bank to arrange the transfer at no cost for the beneficiary. Bank charges, if any, are at the participant's expense. To guarantee your regis-

tration, enclose a copy of your bank transfer.

Cancellations: Refunds of 50% will be made if a written request is received before October 23, 1992. No refunds will be made for cancellations received after this date. In case of symposium cancellation for reasons beyond its control, AFCET limits its liability to the registration fees already paid.

Proceedings: ESORICS 92 proceedings will be distributed on-site to registered participants. Extra copies of ESORICS 92 and ESORICS 90 proceedings will be sold on-site.

Languages: English and French, with simultaneous translation.

Social Event: A dinner banquet will be offered to all registered participants on Tuesday, November 24, 1992. For accompanying persons, banquet price is 250 FF.

Post-Symposium Tour: A visit (by bus) of Toulouse, the medieval city of Carcassonne and their region will be organized on Thursday, November 26, 1992. If interested, please tick the corresponding box on the registration form to receive tour information.

Travel Discounts: About 35% reduction for some Air Inter domestic return flights can be obtained for the Symposium dates. Please tick the appropriate box on the registration form to receive your discount voucher.

Hotel Reservations: There are many hotels in Toulouse in every category. A list of hotels, within walking distance from Hotel Palladia and offering special prices to ESORICS 92 participants, is given at the end of this message. For your reservation, please contact DIRECTLY the hotel of your choice; do not forget to mention ESORICS 92.

Local Organization: Marie-Therese Ippolito, LAAS-CNRS, 7 avenue du Colonel Roche, 31077 Toulouse (France), telephone: +33 61 33 62 74, fax: +33 61 55 35 77, E-mail: esorics@laas.fr.

### **REGISTRATION FORM**

To be sent to: AFCET - ESORICS 92 156, boulevard Pereire 75017 Paris (France) Fax : +33 1 42 67 93 12 Telephone: +33 1 47 66 24 19

(Please print) Name: First Name: Company: Address:

Country: Telephone : Fax : Nb of invoices requested: Invoice(s) to be sent to: Air Inter Discount [] Please send me an Air Inter discount voucher Post-Symposium Tour [] Please send me tour information **Poster Session** [] I wish to present a poster and I enclose its description. FEE (18.6% VAT included): Member: AFCET [] BCS [] GI [] IEE [] NGI [] Before October 24, 1992 : 3000 FF [ ] After October 23, 1992 : 3500 FF [ ] Non member: Before October 24, 1992 : 3300 FF [] After October 23, 1992 : 3800 FF [ ] Accompanying persons for banquet: x 250 FF TOTAL : FF PAYMENT (enclosed): Banker's draft [] Purchase order [] Credit Card Authorization: I duly authorize you to charge my Visa Intl [] MasterCard [] Expiration : Card Number: Card holder name: Signature: Date :

HOTEL LIST

For all reservations, contact DIRECTLY the hotel of your choice, mentioning ESORICS 92, and confirm your reservation by fax or telex.

Palladia \*\*\*\* 271 avenue de Grande Bretagne, 31300 Toulouse telephone : +33 62 120 120 fax : +33 62 120 121 single 490 FF, breakfast 70 FF (Free shuttle available on request from the airport)

#### Dotel \*\*\*

Avenue des Arenes Romaines, 31300 Toulouse telephone : +33 61 83 83 fax : +33 61 31 00 10 single 320 FF, breakfast included (Free shuttle available on request from the airport)

Novotel Toulouse Purpan \*\*\* 23 Impasse Maubec, 31300 Toulouse telephone : +33 61 49 34 10 fax : +33 61 49 63 37 single 430 FF, breakfast 47 FF (Free shuttle available on request from the airport)

Le Grande Bretagne \*\*\* 300 avenue de Grande Bretagne, 31300 Toulouse telephone : +33 61 31 84 85 fax : +33 61 31 87 12 single 390 FF, breakfast included

Campanile Purpan \*\* 33 route de Bayonne, 31300 Toulouse telephone : +33 61 31 09 09 fax : +33 61 31 09 10 single 240 FF, breakfast 29 FF

Gascogne \*\* 25 allees Charles de Fitte, 31300 Toulouse telephone : +33 61 59 27 44 telex : 521090F single 230 FF, breakfast 35 FF (3 km from Hotel Palladia, bus 14 "Saint-Cyprien" stop)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Simon Marshall <S.Marshall@sequent.cc.hull.ac.uk> Sat, 24 Oct 1992 10:55:28 +0000

From Sat 24 Oct 1992 'Guardian', no author given. It is perhaps not too surprising that this has not received the attention that it deserves, given the political situation in the UK at the moment. The British Government is currently in the process of lurching from one crisis to the next. [See Brian Randell's contribution in <u>RISKS-13.44</u> for background. PGN]

Computer software blamed as RAF pilot bombs Ark Royal.

An RAF Harrier jump-jet pilot on exchange with the Royal Navy bombed the carrier Ark Royal, injuring five crew, because of a computer software anomaly, it was disclosed yesterday. Four of the injured have returned to work following the [20 April 1992] incident when the 28lb practice bomb tore through the flight deck and exploded in one of the mess decks. The fifth ... is still receiving medical treatment.

The incident happened when four Sea Harriers were practicing dropping bombs on a target towed 600 yards behind Ark Royal during training .... The RAF Flight Lieutenant, described as highly experienced, lost radar contact twice with the ship. He 'locked on' for a third time just seconds before going into the loft manoeuvre. He did not know that the automatic aim-off was not programmed to cut in within such a short period of time because of an anomaly in the computer software. The bomb was aimed at the ship and not the target. The pilot will receive a formal warning and training using loft-mode attacks has been `put into abeyance'."

What interested me in particular was that, in a roundabout way, the pilot is being faulted, even though the software is blamed. It is worrying that the evaluation of the software (which I assume took place) did not pick this up. Of course, it could well be that the real problem was much more complicated than the article suggests. It would not be the first time the press has simplified a story involving modern technology. Does anyone know more on this? It does, however, bring home the reality that computers control life and death situations.

Simon Marshall, Dept. of Computer Science, University of Hull, Hull HU6 7RX, UK Email: S.Marshall@Hull.ac.uk Phone: +44 482 465181 Fax: 466666

# ✓ Erased Disk used against Brazilian President

Geraldo Xexeo <xexeo@dxcern.cern.ch> Thu, 22 Oct 1992 18:58:52 GMT

In the investigation of the process against the Brazilian President (Fernando Collor de Mello), the Federal Police found (and confiscated) an IBM-PC clone in the enterprises of Paulo Cesar Farias.

In the hard disk of this computer were found dozens of indications of the corruption of Collor de Mello and P.C. Farias.

The "folklore" that runs in Brazil now is that the disks were actually erased, but the FP bought in USA a software that allowed the examination of the disk and the recovery of the files. It seems that this tale is true.

I would like to know which software was used, and what kind of work the FP did.

Jerry / Xexeo

Geraldo Xexeo, CERN - PPE Division, 1211 Geneve 23, Switzerland FAX: (41)(22)785-0207 xexeo@dxcern.cern.ch gxexeo@cernvm.bitnet

### Mathematicski washington washi

Alan Wexelblat <wex@MEDIA-LAB.MEDIA.MIT.EDU> Tue, 20 Oct 92 00:15:02 -0400

Date: Mon, 19 Oct 92 23:49:18 -0400 From: Doug Humphrey <digex@ACCESS.DIGEX.COM> Subject: .0045 mbits/sec

Article <7610172337.AA19083@nisc.jnvc.net> Oct 17 23:37 Subject: T3 Cable Cut From: martin@NISC.JNVC.NET (Steve Martin)

This is to inform you that Merit (NSF) has experienced a fiber cut in East Orange, New Jersey. As a result of this, JNvCnet's T3 access to the NSF net is temporarily out of service till repairs can be made.

All traffic to the NSF net is now being routed through the 9.6k backbone node and will be returned to the T3 as soon as possible.

### Kisks in Banking, Translation, etc.

<cent@mc.lcs.mit.edu> Thu, 22 Oct 92 23:24:34 EDT

[The following message came from Pandora Berman at MIT via Jerry Leichter <leichter@lrw.com>, John Robinson <jr@ksr.com>, Clark M. Baker) <cmb>, and originally from Paul M. Wexelblat <wex@cs.ulowell.edu>, who noted the original CACM item ... PGN]

I stumbled across this little item in the current (October 1992) CACM:

BANKS UNDERDRAWN... The banking industry spent over a billion dollars on technology last year, yet they are not even close to employing leading-edge tools. A new survey ... indicates that over 75% of bank computer programs are still written in Cobol and 84% of banking software is designed for mainframes, not PCs. Moreover, 80% of the software used by banks is over six years old and only 37% of their locations are networked. The report reveals most banks are simply not investigating new advances in computer applications. [Communications of the ACM, Vol 35, No 10, NEWSTRACK, p.9]

Here is a rough translation:

BANKS CONSERVATIVE... The banking industry spent over a billion dollars on technology that works, rather than the latest glitzy play toy. A new survey ... indicates that over 75% of bank computer programs are written in a language appropriate to the task as opposed to trying to force their models into the latest Object Oriented fad and 84% of banking software is designed

to run on systems that have low mean time between failures, juggle hundreds of users, handle huge databases, and push megabytes at high rates, not tiny little machines that crash with great regularity, are designed for a single user, if even that, have minuscule disks, and have bandwidth the approximating that of a sclerotic soda straw. Moreover, 80% of the software used by banks has been fairly well debugged and only 37% of their locations are open to attack by thirteen year olds with modems and a lot of time on their hands. The report reveals most banks are simply not chasing the latest fad in confuser science and piddling their money away on recoding working applications unnecessarily.

Paul Wexelblat

## Ke: 15th National Computer Security Conference (<u>RISKS-13.85</u>)

Dorothy Denning <denning@cs.cosc.georgetown.edu> Tue, 20 Oct 92 14:41:43 EDT

## David Willcox said

Dorothy Denning suggested that anyone using high-level encryption over a public network be required to register their encryption keys with some agency. This agency would then distribute the keys when an appropriate court order was presented. The risks of this are fairly obvious.

I believe this risk can be reduced to about zero. For example, using a public-key system, your key could be encrypted under the public key belonging to, say, the Justice Dept. The encrypted key would be given to and held by an independent agency. But, the key could be decrypted only by Justice. Thus, if somone gains access to a key held by the key agency, they wouldn't be able to decrypt it.

To use a key, law enforcers would have to go through these steps:

- 1. Get a court order.
- 2. Submit the court order to the key agency and get the encrypted key.
- 3. Deliver the encrypted key to Justice with the court order; get back the plaintext key.
- 4. Take the court order to the service provider in order to activate the tap and get the bits.
- 5. Listen in and decrypt the communications.

I believe this scheme is pretty tight. Silvio Micali has evidently invented another method of safeguarding the keys in a registry, called "fair cryptography", but I don't know the details.

Dorothy Denning

### KE: Vote Early, Vote Often

"Louis B. Moore" < lbmoore@tchden.org>

#### Tue, 20 Oct 1992 11:09:22 MDT

>It took the action of citizens banding together to file a civil lawsuit to halt >the abuses after their complaints were rebuffed by the Colorado secretary of >state's office and the local district attorney.

There is an interesting point related to this particular story. The Colorado Secretary of State does not have criminal powers. So in the case of vote fraud like that in Costillo County, the Secretary of State may have to turn the case over to the District Attorney. The District Attorney may have been elected with the aid of the vote fraud (s)he is supposed to prosecute. The other choice of prosecuting authority would be the Attorney General (depending on who had jurisdiction), another elected official.

It is difficult to see how telephone voting will do anything but further exploit existing problems in authenticating voters and prosecuting vote fraud.

Louis B. Moore, Systems Programmer, The Children's Hospital of Denver Denver, Colorado USA 80218 lbmoore@tchden.org +1 303 837 2513

# 🗡 T\*p S\*cr\*t

Berry Kercheval <berry@athos.pei.com> Wed, 21 Oct 92 15:34:30 PDT

"Anonymous" mentions in <u>RISKS DIGEST 13.84</u> that the Department of Defense conducted an investigation when an message marked "T\*p S\*cr\*t" was found on an unclassified computer system. (The asterisks are a way of ensuring that the investigation is not triggered by the words in \*his\* message, I guess.)

I don't think merely putting the words "Top Secret" in a message is the problem; putting it in such a way that it appears to be classified data \*is\*.

I have, in the past, held both Department of Energy and Department of Defense clearances, and if I learned anything it is that the security personnel of both agencies take their jobs very seriously and do not have much of a sense of humor where security violations are concerned.

In my initial briefings for these clearances it was emphasized that classified information must be strictly controlled, and in fact we were given specific procedures for what to do if we found unattended classified documents lying around.

It appears that [the author] thinks that the "system wide disclaimers that said systems are not to be used for classified work" should have been sufficient to prevent action. I feel that the exact reverse is true -- the appearance of an APPARENTLY classified message on an insecure\* computer is exactly the kind of security violation that needs to be investigated immediately.

In fact, I can remember one company that sent out "Top Secret" press releases to their customers -- which included some DoE and DoD sites -- getting an

unpleasant visit from men with dark suits and sunglasses that didn't smile much. (The gist was "Don't \*do\* that".) --berry

## M Book Review: The Hacker Crackdown

David Barker-Plummer <plummer@cs.swarthmore.edu> Sat, 24 Oct 1992 12:06:23 -0400

"The Hacker Crackdown: Law and Disorder on the Electronic Frontier", Bruce Sterling, Bantam Books, November 1992, ISBN 0-553-08058-X, 328pp, US\$23.

Book Review by Dave Barker-Plummer (plummer@cs.swarthmore.edu)

"The Hacker Crackdown" is Bruce Sterling's term for a series of seizures of computer equipment which took place during the summer of 1990. The circumstances surrounding these raids, the individuals and communities affected by them, and the consequences for the computing community and society at large, are the subjects of this book.

Sterling, a cyberpunk author, is at his best when he is telling stories. He adopts a revelatory style and writes in a tone of wonder and bemusement as events take one unexpected turn after another. Particularly intriguing is his telling of the Craig Neidorf/Knight Lightning story. Neidorf was prosecuted for electronically distributing an edited version of a document copied without permission from a BellSouth computer. Sterling documents the history of the document as it was sent across the Internet many times, its publication in the "Phrack" newsletter, the arrest of Neidorf, the charges against him and the eventual collapse of the trial. As the story unfolds, one realises that truth is indeed stranger than even Sterling's bleak cyberpunk fiction.

There are many other stories in the book: the story of Steve Jackson, whose legitimate games company was raided under sealed warrant, and all of his computers seized; the story of The Legion of Doom, a group of hackers who assemble in cyberspace to brag about breaking into computers and sharing stolen access codes and credit card numbers; the story of the founding of the Electronic Frontier Foundation by Mitch Kapor, author of Lotus 1-2-3, and John Perry Barlow, sometime lyricist for The Grateful Dead; and closing the book, the story of the Computers, Privacy and Freedom conference of 1992, in which hackers, law enforcement, and civil libertarian groups met to talk about these issues with unprecedented openness.

Sterling attempts to make these stories take second place to the culture, or more correctly cultures, of cyberspace. He chooses to structure his book in four main parts, each dealing with one of these subcultures. While hacker stories have been told before, this examination of cultures has been neglected, and Sterling is to be praised for attempting it. However, Sterling does not seem to comfortable in his self-appointed role. Try as he might, the events keep overtaking the people, and the book ends up feeling somewhat confused ---but then the whole subject is rife with confusion: cultural, technical and ethical. Although Sterling fails to give it the emphasis it deserves, the main theme of this book is power. In the first part of the book "Crashing the System", Sterling describes the power of the telephone companies. From the fledgling technology of the telephone, through the rise of AT&T, and the significant role that it played in government and industry, to the break up of the Baby Bells. The picture that Sterling paints of the contemporary telcos is that of a power base that is under threat, and which is struggling to preserve its grip on the power that is being threatened by the more widespread availability of technology, not to mention the breaking of the economic monopoly. Lest this sounds like dull reading --- there's not a sentence in this book that can be described as dull --- I should mention that Sterling brings this history to life by taking us in detail through the duties of a switchboard operator, and observing that in the early days of the telephone teenage boys often played this role until they were found to be "hacking", when they were ejected from the system. There are intriguing parallels between the time just after the introduction of the telephone --- which Sterling identifies as the creation of cyberspace --- and the contemporary era, which represents the settling of that "place".

The second section of the book, "The Digital Underground", documents the hacker subculture. Sterling steers a journalistic middle course: on the one hand stressing the illegality of hacking and debunking the myth of the talented genius, while at the same time pointing out that the typical hacker is not a hardened criminal but a teenage boy. Sterling explains the feeling of technical power for a hacker when he uses a computer to break into a voice mail PBX, or to break into a password protected system, to gain access to hitherto inaccessible regions of cyberspace. Sterling makes much of the isolation and cultural powerlessness of hackers: they are typically teenage boys who grew up in the Reagan era and have come to believe that all institutions are corrupt, and who see their computer and modem as weapons against those institutions, even if it is only to steal insignificant documents, or do no more than irritate those institutions. He also describes the material available on "underground" BBSs, illustrating the anarchistic stances adopted by these elite children of elite families, and debunks the myth that there are "gangs" of hackers working in concerted effort to bring about the downfall of the technocracy as we know it, but asserts that their's is typically a solitary "game". This isolation leads to their need to brag of their exploits to other hackers, in order to build a reputation, and often thereby to their swift arrest. Isolation also accounts for the fact that almost every hacker arrested cooperated fully and informed on his contacts in cyberspace. There is no hacker community, Sterling implies, and no honour among hackers.

In the third section, "Law and Order", Sterling describes the world of the law enforcement officers. If one thing comes through from this picture it is that the law enforcement agencies in this country were/are ill-prepared to investigate and prosecute computer crime. Sterling remarks that he, a not particularly computer-literate, author has more computer power in his home than the typical computer law enforcement officer (of 1990). Sterling describes the modus operandi of a typical hacker bust, the seizure of everything that looks like it might be relevant including CDs (that might store data and be disguised as music CDs), and Sony Walkmen (because they are electronics, I guess). In his article "Crime and Puzzlement", John Perry Barlow writes "In fairness, one can imagine the government's problem. This is all pretty magical stuff to them. If I were trying to terminate the operations of a witch coven, I'd probably seize everything in sight. How would I tell the ordinary household brooms from the getaway vehicles?". While Sterling's description of the problems facing the under-funded, under-equipped and under-skilled government agencies is sympathetic, he does not seek to justify the excesses in the events of 1990. He carefully makes and maintains the distinction between hackers from legitimate computer users, and describes how members of both of these groups were equally punished by the Hacker Crackdown.

Finally, in "The Civil Libertarians" Sterling describes the response of the Silicon Valley and Austin computer culture to the strange events of the hacker crackdown, which culminated in the formation of the Electronic Frontier Foundation. In this very upbeat section, Sterling describes how the computer elite used their technological power to network and organize, to seize the public relations advantage, to file suit in defense of Steve Jackson and Craig Niedorf and to set themselves up to defend civil liberties in cyberspace. In the view of the civil libertarians, the hacker crackdown was the first skirmish in the battle for control of cyberspace. The Electronic Frontier is a new "place" that is currently being populated and the rules that will govern this place are up for grabs. The civil libertarians are concerned to guarantee important rights for the citizenry of cyberspace, in particular: freedom of expression, freedom of association and privacy: in effect a constitution for cyberspace.

"The Hacker Crackdown" taught me much about the events of the early 90s and it is entertaining and provoking by turns. I recommend it highly, for its discussion of the contemporary struggle for technological power, illustrated by unbelievable, but true, stories of law and disorder on the electronic frontier.

### \* filling station POS terminals: credit card users beware!

Steve Summit <scs@adam.mit.edu> Wed, 21 Oct 92 13:08:15 -0400

Today I bought gasoline and discovered that the station had some fancy new pumps with credit card readers built right in. You can drive up, insert your card, pump gas, and drive away, without even dealing with a clerk. The pump prints a little receipt when you're finished.

The problem is the receipt. It comes out behind a small clear plastic door (presumably the door is to protect the printer from the weather); you have to slide it open so that you can fish the receipt out, slightly awkwardly, with your finger. If you don't notice the receipt at all, or if you're in a hurry, or if you aren't in the habit of saving receipts anyway, you could easily leave it behind.

On the receipt is printed not only your credit card number and type of card (VISA, MC, etc.), but also your full name, as retrieved from the magstripe.

If Bonnie S. Thomason happens to read this, you forgot your receipt after buying 13.855 gallons of unleaded at 7:59 this morning, but I promise I won't use or disclose your credit card number. Wandering around checking these receipt slots would be reminiscent of wandering around checking pay telephone coin return slots, but potentially much more lucrative.

Besides RISKS, I'm writing a letter to the oil company in question today.

[This is of course an old problem for RISKS readers, but it is perhaps worth including here as a reminder that it recurs continually. PGN]

## M Int Workshop on Fault and Error Models of Failures in Comp Sys.

"Ram Chillarege (914) 784 7375" <ramchill@watson.ibm.com> Fri, 23 Oct 92 08:51:13 EDT

Abstract Submission : NOVEMBER 2, 1992 Deadline Approaching : \*\*\*\*\*\*\*\*\*\*\*\*

**Call for Participation** 

International Workshop on Fault and Error Models of Failures in Computer Systems

January 25 - 26, 1993 o Palm Beach o Florida

-----

Sponsor The IEEE Computer Society and IEEE Technical Committee on Fault-Tolerant Computing

Dates

Abstract Deadline:November 2, 1992Acceptance Notification:December 15, 1992Session Foils/Agenda:January 8, 1993

#### Scope

The importance of understanding Computer System failures, in terms of their fault and error models, failure patterns, and characteristics cannot be over emphasized. This understanding is critical in influencing the research and practice of fault-tolerant computing. It is the kernel upon which evaluation methods, experimental verification, modeling, algorithms and techniques are developed. In recent years the relative mix in the causes of outage has shifted from what it was a decade ago. Studies indicate the dominance of software as a cause of outage, closely followed by maintenance and environment. However, the industry lacks data and understanding of faults, errors and failures in these dimensions - severely impacting the progress of fault-tolerant computing as a research discipline and a practice.

This workshop is intended to bring together experts from industry, academia, and government. The goal is to develop the needed insight, define and

calibrate models, and gain knowledge to guide research and practice in fault-tolerant computing. This workshop will be highly interactive. It will be run as a workshop, and will not have a conference flavor. It is intended that at the end of the two day meeting, there will evolve a substantial accomplishment towards these goals. These results are intended to be the starting point of a sequel to this workshop, on fault-injection. The fault-injection workshop, also sponsored by the Technical Committee on Fault-Tolerant Computing, is planned to be held in Sweden in June 1993.

#### Submission

To participate in this workshop, submit seven copies (or use email) of a two page abstract describing the contribution you will make to the workshop. The program committee will review the abstracts and notify you of your acceptance. To enhance interaction the attendance at the workshop will be limited to a maximum of fifty.

#### Workshop Chair

Ram Chillarege, IBM Research, USA

#### **Program Committee**

Bob Horst - Tandem Computers, USA Ravi Iyer - University of Illinois, USA Karama Kanoun - LAAS-CNRS, France Dan Siewiorek - Carnegie Mellon, USA Yoshihiro Tohma - Tokyo Institute, Japan Jan Torin - Chalmers University, Sweden

### Submit Abstracts to

Ram Chillarege IBM T. J. Watson Research Center 30 Saw Mill River Road Hawthorne, NY 10532, USA (914) 784-7375 Fax: (914) 784-6201 email: ramchill@watson.ibm.com

#### Important Dates

Submission Deadline:November 2, 1992Acceptance Notification:December 15, 1992Session Foils/Agenda:January 8, 1993

Ex Officio

Jacob Abraham, FTC-TC Chair, University of Texas, Austin, USA

✓ Call for papers, Computer Security Foundations Workshop VI

Catherine A. Meadows <meadows@itd.nrl.navy.mil> Fri, 23 Oct 92 18:59:51 EDT

CALL FOR PAPERS COMPUTER SECURITY FOUNDATIONS WORKSHOP VI June 15-17, 1993 Franconia, New Hampshire Sponsored by the IEEE Computer Society

The purpose of this workshop is to bring together researchers in computer science to examine foundational issues in computer security, with emphasis on formal models that provide a framework for theories of security and techniques for verifying security as defined by these theories.

We are interested both in papers that describe new results in the theory of computer security and in papers, panels, and working group exercises that explore open questions and raise fundamental concerns about current theories of security. Possible topics include access control, covert channels, information flow, database security, secure protocols, verification techniques, integrity and availability models, interactions of computer security requirements with other system requirements such as dependability and timing, and the role of formal methods in computer security.

The proceedings are published by the IEEE Computer Society and will be available at the workshop. Selected papers will be invited for publication in a special issue of the Journal of Computer Security.

Instructions for Participants: Workshop attendance will be limited to thirty-five participants. Prospective participants should send four copies of a paper (limit 7500 words), panel proposal, or working group exercise to Catherine Meadows, Program Chair, at the address below. Please provide email addresses and telephone numbers (voice and fax) for all authors. The contact author should be clearly identified.

IMPORTANT DATES: Author's submission: January 29, 1993 Notification of acceptance: March 10, 1993 Camera-ready final papers: April 9, 1993

**Program Committee** 

Marshall Abrams, MITREJohn Mclean, NRLSimon Foley, University College, CorkJonathan Millen, MITRELi Gong, ORARobert Morris, DoDJames Gray, NRLRavi Sandhu, GMUJeremy Jacob, OxfordMarv Schaefer, CTA

For further information contact:

General Chair Ravi S. Sandhu ISSE Department George Mason University Fairfax, VA 22030-4444 +1 703-993-1659 sandhu@sitevax.gmu.edu

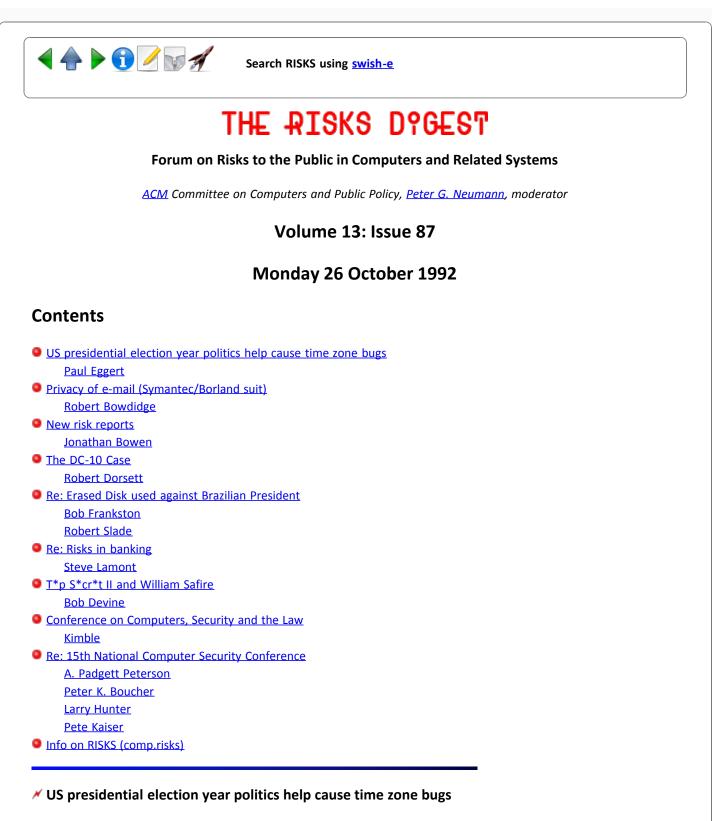
Program Chair Catherine Meadows Code 5543 Naval Research Laboratory Washington, DC 20375 +1 202-767-3490 meadows@itd.nrl.navy.mil

Publications Chair Joshua Guttman The MITRE Corporation Burlington Road Bedford, MA 01730 +1 617-271-2654 guttman@linus.mitre.org



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Paul Eggert <eggert@twinsun.com> Mon, 26 Oct 92 14:47:57 PST

Several people on the west coast of the US reported that their Unix systems failed to switch from daylight savings time to standard time yesterday, 25 October 1992. The reason? When they originally configured their systems, they were asked to choose one of the following time zone rules:

...

US/Alaska US/Central US/Hawaii US/Pacific US/Aleutian US/East-Indiana US/Michigan US/Pacific-New US/Arizona US/Eastern US/Mountain US/Samoa

Some people chose `US/Pacific-New' instead of `US/Pacific'. After all, who wants the old version when you can have the new version?

Unfortunately, 'US/Pacific-New' stands for ``Pacific Presidential Election Time'', which was passed by the House in April 1989 but never signed into law. In presidential election years, this rule would have delayed the PDT-to-PST switchover until after the election, to lessen the effect of broadcast news election projections on last-minute west-coast voters. Thus, US/Pacific-New and US/Pacific have always been identical -- until yesterday.

This problem comes from combining Arthur David Olson's deservedly popular time zone software (which you can FTP from elsie.nci.nih.gov in pub/tz92b.tar.Z) with some overly terse vendor-supplied installation procedures. No doubt Olson did not use a more informative name like `US/Pacific-Presidential-Election' because of the 14-character file name length limit in many Unix file systems. In view of yesterday's experience, though, it seems unwise to make the hypothetical choice available under any name, since it gives free rein to Murphy's Law.

# Privacy of e-mail (Symantec/Borland suit)

Robert Bowdidge <bowdidge@cs.UCSD.EDU> Tue, 6 Oct 92 12:54:30 -0700

In the Los Angeles Times business section on Monday, 5 October 1992, there was an article describing some of the difficulties of Symantec, a publisher of software for the Macintosh and IBM-PC markets. One of the more interesting situations for the company was a criminal complaint and civil suit filed by Borland International charging a former Borland vice president with passing trade secrets.

### >From the article:

(Eugene) Wang, disappointed after a management reshuffle two months earlier, resigned from Borland earlier the same day [that Symantec announced he had been hired as a vice president]. Acting on a tip, Borland officials searched records of electronic mail that Wang had sent via MCI Mail. They found ten messages he had sent to Eubanks and others that allegedly contained proprietary information on Borland's product plans.

Normally, that might lead to a civil suit. Such actions have become relatively common in an industry where the expertise of a few people is often a company's key asset.

But Borland took matters a step further, filing a criminal complaint with the Scotts Valley Police Department in addition to a civil suit. Police said they found the information in the messages sufficient grounds to seek a search warrant [for Symantec's offices and Wang's home.]...

Legal experts who aren't involved in the case don't know what to make of it.

``At first blush, it seems like they (Borland) must have had some pretty good evidence,'' said Kaufman of [Brobeck, Phleger, and Harrison, a San Francisco law firm]. ``But it's bizarre -- Wang, a premier computer scientist, doesn't know that when you use MCI mail, it's recorded? It's a very strange set of facts.

[Yet another reason to encrypt my mail... Robert Bowdidge bowdidge@cs.ucsd.edu]

## New risk reports

<Jonathan.Bowen@prg.ox.ac.uk> Mon, 26 Oct 92 14:46:11 GMT

There is an article on risk in today's (Monday, 26 October 1992) UK Independent newspaper (p14) which RISKS readers may find interesting entitled "The chances of being run over by a bus" by Tom Wilkie. It advertises two reports which sound as if they are worth looking at:

"The Tolerability of Risk from Nuclear Power Stations", HMSO, PO Box 276, London SW8 5DT, UK. (12 pounds sterling.)

"Risk: Analysis, Perception and Management", The Royal Society, 6 Carlton House Terrace, London SW1Y 5AG, UK. (15.50 pounds sterling.)

The latter values "a statistical life" at 2-3 millions pounds sterling (c \$4 million) in that this is the sort of amount of money that should be spent on saving one life. However the article states that John MacGregor, the Secretary of State for Transport, for his department values a life at only around 500,000 pounds sterling.

Jonathan Bowen, Oxford University

(Of course, the value of a human life in the UK has been devalued by about 10% recently. :-)

# M The DC-10 Case [also in sci.aeronautics, rec.travel.air]

Robert Dorsett <rdd@cactus.org> Fri, 9 Oct 92 01:17:11 CDT

Ran across this. It looks like a nice little anthology, covering many aspects of the DC-10. Probably worth it for the NTSB reports alone (\$20 each from NTIS). I haven't read the more "thematic" articles, though, and no endorsement is meant or implied. Robert Dorsett ...cs.utexas.edu!cactus.org!rdd

Title: The DC-10 Case Subtitle: A study in applied ethics, technology, and society. Editors: John H. Fielder and Douglas Birsch Publisher: State University of New York Press Date: 1992 Pages: 346

# ISBN: 0-7914-1087-0 (hardcover) 0-7914-1088-9 (paper) Illustrated.

#### CONTENTS:

Preface Introduction Ethical Analysis of Case Studies/John H. Fielder

HISTORY AND EARLY WARNINGS

- 1. Regulatory and Institutional Framework
- 2. High Risks, Sinking Fortunes/John Newhouse
- 3. Floors, Doors, Latches and Locks/John Fielder
- 4. The 1970 Ground Testing Incident/Paul Eddy, Elaine Potter, Bruce Page
- 5. National Transportation Safety Board Report on the Windsor Incident
- 6. The Applegate Memorandum/Paul Eddy, Elaine Potter, Bruce Page
- 7. Fat, Dumb and Happy: The Failure of the FAA/Paul Eddy, Elaine Potter, Bruce Page
- 8. Compliance with Service Bulletin SB 52-37
- 9. Conclusions of the US Senate Oversight Hearings and Investigation of the DC-10 Aircraft
- THE 1974 PARIS CRASH
- 10. French Government Report on the 1974 Paris Crash
- 11. Engineers Who Kill: Professional Ethics and the Paramountcy of Public Safety/Kenneth Kipnis
- 12. Whistleblowing, Ethical Obligation, and the DC-10/Douglas Birsch
- 13. What is Hamlet to McDonnell Douglas or McDonnell Douglas to Hamlet?: DC-10/Peter French

Commentary/Homer Stewell

14. Statement of John C. Brizendine, President, Douglas Aircraft Company, McDonnell Douglas Corporation

THE 1979 CHICAGO CRASH

15. National Transportation Safety Board Report on the 1979 Chicago Crash

- 16. The DC-10: A Special Report/McDonnell Douglas
- 17. Two Models of Professional Responsibility/Martin Curd and Larry May

THE 1989 SIOUX CITY CRASH

- 18. National Transportation Safety Board Report on the 1989 Sioux City Crash
- 19. The 1989 Sioux City Crash/John Fielder
- 20. Statement of Ralph Nader
- 21. Aviation Safety: Management Improvement Needed in FAA's Airworthiness Directive Program
- 22. The FAA, the Carriers, and Safety/Charles Perrow
- 23. International Airline Passengers Association Critique of the DC-10
- 24. Moral Responsibility for Engineers/Kenneth D. Alpern

Commentary/Andrew Oldenquist

Commentary/Samuel C. Florman

Select Bibliography

**IEEE Code of Ethics** 

Index

Back Cover:

"Designed as a textbook for courses in ethics, this book provides the material needed to understand the accidents in which more than 700 people were killed--accidents that many believe were the result of unethical actions and inactions by individuals, organizations, and government agencies. An introduction to ethical analysis and discussions of the ethical responsibilities involved are also provided. The case study offers material for a sustained inquiry into every level of ethical responsibility reflecting the rich complexity of actual events.

"\_The DC-10 Case\_ presents these issues through a collection of original and published articles, excerpts from official accident reports, congressional hearings, and other writings on the DC-10. The authors allow the readers to examine the ethical issues of airline safety as they actually occur, taking account of the circumstances in which they arise.

"John H. Fielder is is Professor and Douglas Birsch is Assistant Professor of Philosophy at Villanova University."

# 🗡 Re: Erased Disk used against Brazilian President

<Bob\_Frankston@frankston.com> Sun 25 Oct 1992 01:57 -0400

Of course, as RISKS readers know, getting rid of information is very difficult. On the PC erase only erases the name of a file not the contents. With proper backup, as Oliver North discovered, it is very hard to remove all copies of data. There are also other caches such as email pools where one might be able to retrieve recent data.

There is a more general issue of living in a society with a very good memory. It is one thing to knowingly do something illegal and leaving a trail. A more subtle danger is a changing society that might look back at an innocuous act and ex post facto, decide it was reprehensible.

# Ke: Brazilian Presidential Erased Disks (<u>RISKS-13.86</u>)

Robert Slade <rslade@sfu.ca> Mon, 26 Oct 1992 20:05:30 GMT

The software used here is probably very simple. When a computer file is "erased", actually only the directory entry is changed, and the sectors used are marked as again being available for use. The file can easily be "undeleted": numerous utilities exist for this purpose, including (I am assuming, from the original posting, that the computer in question uses MS-DOS) one that is part of the MS-DOS 5 system. In fact, such utilities need not be used: if no changes have been made on the disk, the FAT can be changed manually with a sector editing program.

If the file cannot be "undeleted" in this manner, part of the file may still exist on the disk, and can be read with a sector editor or viewer. (I recently checked a diskette with the CHKDSK utility, and found portions of files that had been deleted three or four years ago. This particular disk has been in daily use with three or four large files being written to it each day.)

The fact that files are not actually "destroyed" has come as a shock to a number of people. I seem to recall that this fact had some significance to Ollie North. Also, Prodigy scared the pants off some people by creating a large "swap" file area on disk without "clearing" it first. Portions of deleted files were, of course, found within it, leading to (somewhat unjustified) charges that Prodigy was somehow violating system security.

The fact that erased files may still physically exist is one that some antiviral programs try to address. When an infected file cannot be "disinfected", some antivirals will delete the existing file ... and then overwrite the area previously occupied with standard characters. There are utility programs which will do this with files you wish to keep secret: some make five or more passes with different characters each time.

Vancouver Institute for Research into User Security, Canada V7K 2G6

ROBERTS@decus.ca rslade@cue.bc.ca p1@CyberStore.ca 604-526-3676

[Also noted by ray@philmtl.philips.ca (Ray Dunn). PGN]

## Re: Risks in banking

Steve Lamont <spl@golgi.ucsd.edu> Sun, 25 Oct 92 15:45:40 -0800

For what its worth and just as a matter of record, I am the original author of the item "Risks in Banking, Translation, etc.," which appeared in <u>RISKS-13.86</u>. It was a submission to a recent issue of Gene Spafford's Yucks Digest mailing list.

Steve Lamont, SciViGuy -- (619) 534-7968 -- spl@szechuan.ucsd.edu UCSD Microscopy and Imaging Resource/UCSD Med School/La Jolla, CA 92093-0608

[Also noted by Paul M. Wexelblat <wex@bigmax.ulowell.edu>. Actually the ORIGINAL AUTHOR was someone unidentified on the CACM staff. Steve was the original contributor, to YUCKS. PGN]

# T\*p S\*cr\*t II and William Safire

<devine@postgres.berkeley.edu> Mon, 26 Oct 92 17:53:53 -0800

Berry Kercheval write:

>In my initial briefings for these clearances it was emphasized that classified >information must be strictly controlled, and in fact we were given specific >procedures for what to do if we found unattended classified documents lying >around.

Political columnist William Safire told the story that he would get his personal documents past government security officers by putting a printed heading on each document. The heading came from a very high security level document that he once saw as part of reporting. All went fine for a long time because he could take his "protected" document that contained his notes into meetings. Unfortunately, one day a security person confiscated the document because he wasn't supposed to have such a highly secret codeword on it!

This is analogous to protective coloration in nature... Bob Devine

# Conference on Computers, Security and the Law

<kimble@minster.york.ac.uk> Thu, 22 Oct 92 15:43:51

COMPUTERS SECURITY AND THE LAW,

A CONFERENCE TO BE HELD AT THE UNIVERSITY OF YORK 31 March - 01 April 1993

The conference will be run by the Department of Computer Science at the University of York in association with the Licensing Executives Society and the Society of Computers and the Law.

The aim of the conference is to highlight some of the important legal issues that surround the use, and abuse, of computer technology in a way that should be accessible to the non-specialist, such as lawyers or computer scientists.

The target audience for the conference are senior managers and others in both public and private sector organisations who wish to improve their knowledge about the legal aspects of buying, using or creating computer related products and services. The conference will be of interest to the police, the civil service, banks, insurance and building societies.

The programme will take place over two consecutive days. The first day will deal with the legal aspects of intellectual property rights, copyright and contract law as it relates to computer products and services. The second day will deal with the topics of computer crime and its prevention, security, data protection and privacy.

The conference dinner will be held at the end of the first day with a keynote speaker who will provide the link between the themes. Delegates will be able to register for either of the two days separately if they wish.

Proceedings of the conference will be published and available to participant after the conference.

FEES: Fees will range from #275 for the full conference to #165 for one day. Discounts are available for early booking.

#### **Provisional Programme**

Day One:

Duy One.					
10.30 - 11.15	Overview of law relating to intellectual property rights				
11.15 - 12.00	Copyright law				
12.00 - 12.45	(Questions & Answers)				
14.00 - 14.45	Computer contracts. (Software)				
14.45 - 15.30	Computer contracts. (Hardware)				
16.00 - 16.45	(Questions & Answers)				
19.00 - 22.00	Conference Dinner and keynote speaker at				
St William's College in York					
Day Two:					
10.00 - 10.45	Computer Crime				
10.45 - 11.30	Damage to programs or data				
11.30 - 12.15	(Questions and Answers)				
13.30 - 14.15	Hacking				
14.15 - 15.00	Data Protection Act, Security & Privacy				
15.30 - 16.15	(Questions and Answers)				

THE UNIVERSITY OF YORK is situated in Heslington, two miles away from the centre of York. The campus has been described as one of the finest examples of

twentieth century English romantic landscape architecture. Its main feature is a large man-made lake supporting a wide variety of wild fowl.

The Department of Computer Science has an international reputation for being at the leading edge of developments in the fields of Software Engineering, Safety Critical Systems, Human Computer Interaction and New Computer Architectures It has recently expanded both its teaching and research to include the many faceted and dynamic field of the application of Information Technology to Business Management and maintains many contacts in both industry and government agencies.

#### LICENSING EXECUTIVES SOCIETY

The Society is committed to providing education and information to present and future users of licensing, and gladly supports the University of York in this conference, which will answer an ever increasing demand in the business and licensing communities for up-to-date information on this important subject.

### SOCIETY OF COMPUTERS AND THE LAW

The Society was founded in 1973 as a forum to promote the effective and profitable use of computer technology for lawyers. The Society informs and promotes interest both in the development of information technology for the practice and teaching of law, as well as in the law relating to computers - not only for Society members but also for members of the public at large.

FURTHER DETAILS FROM: Conference Organiser: Francoise Vassie, Centre for Continuing Education, King's Manor, York, YO1 2EP, The University of York Tel 0904 433900 Fax 0904 433906, E-Mail KIMBLE@UK.AC.YORK.MINSTER

# 15th National Computer Security Conference (Denning, <u>RISKS-13.86</u>)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Sat, 24 Oct 92 17:25:53 -0400

>From: denning@cs.cosc.georgetown.edu (Dorothy Denning)

... >5. Listen in and decrypt the communications.

With all due respect to Mrs. Denning, I suspect that item number five would not be "Listen in and decrypt the communications" but rather "Listen in and discover that a secondary encryption was also used".

Anyone intelligent enough to realize that a process for disclosure existed would be intelligent enough to use the approved scheme to mask the real encryption, or even just to use a different key from the "approved" one if they really had something to hide.

The only advantage to the suggested scheme would be to the "bad guys" since steps 1-5 would have to be processed before the deception would be discovered or is there a suggestion that "someone" should randomly test messages to see if the approved key is sufficient to decrypt ?

Point is, the technology exists to encrypt transmissions, even if it is as

simple as the DE knowing that when I say "stop" I really mean "go". Legislating breakability has about as much chance as commanding the sun to rise in the East: it will appear to be effective only until it is tested.

Padgett

## Ke: (Denning, <u>RISKS-13.86</u>)

"Peter K. Boucher" <boucher@csl.sri.com> Mon, 26 Oct 92 10:52:02 -0800

Dorothy Denning writes:

> I believe this risk

[abuse of encryption keys registered with a government agency] > can be reduced to about zero. For example, using a > public-key system, your key could be encrypted under the public key belonging > to, say, the Justice Dept. The encrypted key would be given to and held by an > independent agency. But, the key could be decrypted only by Justice. Thus, if > someone gains access to a key held by the key agency, they wouldn't be able to > decrypt it.

- 1) Can you trust the criminals to provide the keys to their data and to use those keys (and no others) when transmitting incriminating data? If not, what's the point?
- 2) If you send mangled random data (garbage), can you be prosecuted for not giving the Gov't the proper keys? Will they believe your assertion that your transmission was truly meaningless?
- 3) What exactly are the anticipated benefits of registering keys with a federal agency, and, given your answers to the above, how do they justify the cost and inconvenience of creating such a system?

Peter K. Boucher, Computer Science Lab, SRI International #EL-237 Menlo Park, CA 94025 boucher@csl.sri.com (415) 859-3927

## // (Re: Denning, <u>RISKS-13.86</u>)

Larry Hunter <hunter@nlm.nih.gov> Mon, 26 Oct 92 12:38:23 -0500

In <u>Risks 13.86</u>, Dorothy Denning claims that it is easy to set up a government depository into which all decryption keys for all encrypted messages send over public networks which would be safe from non-court ordered government interception. I must disagree. Her plan is (quoting):

[U]sing a public-key system, your key could be encrypted under the public key belonging to, say, the Justice Dept. The encrypted key would be given to and held by an independent agency. But, the key could be decrypted only by Justice. Thus, if somone gains access to a key held by the key agency, they wouldn't be able to decrypt it.

To use a key, law enforcers would have to go through these steps:

1. Get a court order. ...

However, if the \_Justice Department\_ gains access to a key held by the agency (or the agency's whole database), they would indeed be able to decrypt traffic. For Dr. Denning's scheme to work, I have to trust the "independent" agency not to collude with the Justice Department. I certainly would not trust any executive branch agency not to cooperate with another executive branch agency. It is also extremely unlikely a "key agency" would be formed outside of the Executive. The only precedent I can think of is the Federal Reserve system, and even its independence in circumstances of significant interest to the executive (e.g. interest rates around election time) is suspect.

In my personal opinion, Dr. Denning's proposal does not adequately address the issues raised by socio-political context of her weak encryption scheme. Without extremely stiff penalties and personal liability for illegal decryption in addition to a technical system that identified decrypting parties, it is hard to imagine how any system could require key registration and still offer some protection against nonwarrant government surveillance. The political difficulty of passing legislation that involves the potential for such penalties to be applied to law enforcement officers suggests to me that all "weak" schemes are unlikely to offer such protection.

# \* The "independent agency" to hold cryptokeys

European Technology & Architecture <kaiser@heron.enet.dec.com> Sun, 25 Oct 92 22:54:19 -0800

Dorothy Denning writes:

The encrypted key would be given to and held by an independent agency.

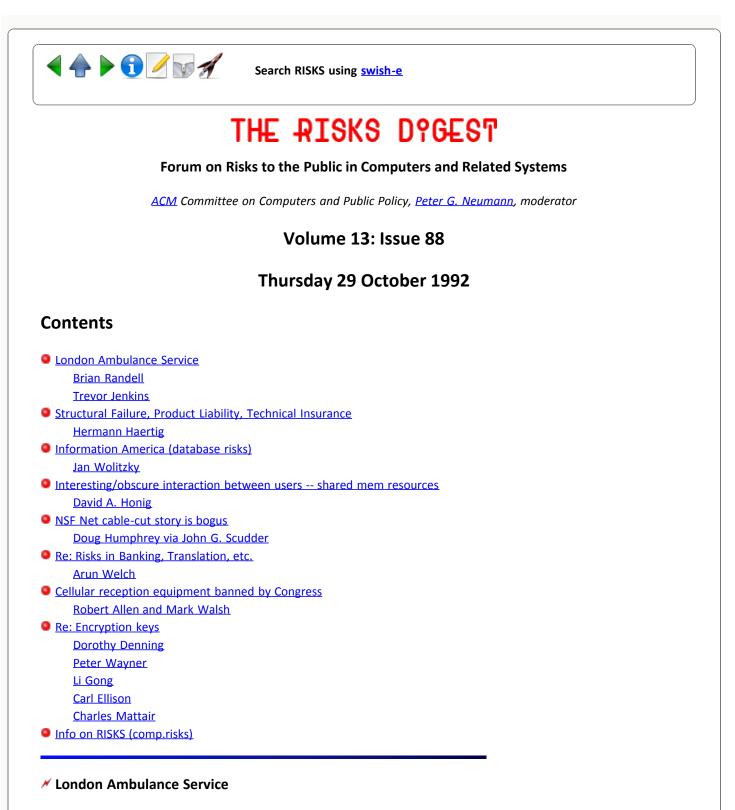
But there is in fact no such agency in the federal government, which means that all such discussion is empty theorizing. Judging the events of the last several decades make me pessimistic that we could ever have one (again?).

\_\_\_Pete kaiser@heron.enet.dec.com +33 92.95.62.97



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<Brian.Randell@newcastle.ac.uk> Thu, 29 Oct 1992 12:38:36 GMT

The top news item in the UK last night on the main BBC television news programmes, and this morning in the national papers, was the trouble at the London Ambulance Service, in particular with their computer-based ambulance dispatching system. (These problems have featured on RISKs before. [Yes, <u>RISKS-13.38</u>, 42, 43]) However previous complaints, warnings and campaigns about delayed ambulance dispatching had had little effect, so that the situation has been allowed to reach a crisis point, with what sound to be credible reports of a number of deaths being caused this week as a result of introducing the latest stage of computerization. No doubt many more stories will follow, but below is the entirety of the front page report in today's Independent. Brian Randell

# AMBULANCE CHIEF QUITS AFTER PATIENTS DIE IN COMPUTER CRASH By Ian MacKinnon and Stephen Goodwin

The Chief executive of the London Ambulance Service resigned yesterday over allegations that up to 20 people may have died because of the collapse of a new computer system controlling emergency calls. Virginia Bottomley, Secretary of Sate for Health, was forced to announce an external inquiry into the 36 hours over Monday and Tuesday which led to delays of up to three hours in ambulances arriving.

Nupe, the public employees' union which represents ambulance staff, said that the resignation of John Wilby was recognition of management failure, but the Government was to blame for years of underfunding. Mrs. Bottomley's response to the "teething troubles" with the 1.5m computer system introduced in stages since January drew angry responses from both backbenches. David Blunkett, Labour health spokesman, demanded that outside managerial expertise be brought in and accused Mrs. Bottomley of failing to respond to the clear signs of crisis which has been building up for months.

Despite union warnings management brought the computer-aided dispatch system fully on stream at 3a.m.on Monday giving cross-London coverage for the first time. The capital had been divided into three sectors - south of the Thames, north-east and north-west - with teams sending ambulances in their area by a combination of two-way radio and telephone, and computer displays in vehicles. Attempts to introduce the system partially in March collapsed.

The full introduction of the computer system effectively did away with the radio and telephone calls to stations, with the computer dispatching crews to answer calls. But within hours, during the morning rush, it became obvious to crews and control room staff that calls were going missing in the system; ambulances were arriving late or doubling up on calls. Distraught emergency callers were also held in a queuing system which failed to put them through for up to 30 minutes.

Chris Humphreys, Nupe's divisional officer, said that it was hard to verify how many people might have died because of the delays but it could be as many as 20. However, the ambulance service contradicted claims that one 14-year-old boy had died of an asthma attach after waiting 45 minutes. It said that the call was dealt with in 28 minutes - although the Patient's Charter has a target of 14 minutes. A man of 83 was also said to have died before the service reverted to the old system at 2p.m. on Tuesday.

Management said initially yesterday that control room staff had been overloaded by the new system as they tried to respond to the extraordinary level of calls. But in the Commons Mrs. Bottomley conceded that the computer system "broke down" and that the old system would remain in operation until the problems had been solved. Martin Gorham, deputy chief executive of South West Thames Regional Health Authority, is to take over from Mr. Wilby until a replacement is found. Mrs. Bottomley said that chief executive of another metropolitan ambulance service would be appointed to head the inquiry, which would be made public as soon as possible. But her responses and earlier failures to act on numerous warnings left MPs dismayed. David Mellor, MP for Putney, called in his first Commons contributions since resigning as Secretary of State for Heritage for "top to bottom reform".

Dept. of Computing Science, The University, Newcastle upon Tyne, NE1 7RU, UK EMAIL = Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

## ✓ London Ambulance Fiasco

Trevor Jenkins <tfj@apusapus.demon.co.uk> Thu, 29 Oct 92 16:48:10 GMT

The UK media have had a field day in the last four days with the inauguration of the new Command and Control System for the London Ambulance Service. The press concentration has centred upon the delays experienced by people calling the service (up to eleven hours in a few cases). One distraught ambulance driver was interviewed and recounted that the police are saying "Nice of you to turn up" and other things. As of 23:00 last night Oct 28 the LAS instigated a backup procedure to ensure that calls were handled in a timely fashion.

Several issues that the press did not cover were:

- o There appears to have been NO backup procedure at all.
- o The design of user interface was inadequate.
- o No consideration was given to system overload was made.

The good news is that the first seems now to have been recitified.

However, the second problem is the one that worries me the most. Much of the TV coverage centred upon shots of the Control Room itself. Wow, this is full of the latest technology---lots of fancy graphic screens showing maps and other goodies. There are trackerballs for the operators to play with. The utilisation of all of this stuff is however flawed. Many times the newscaster quoted operators saying this like:

o there was no way to scroll back through the list of calls to ensure that a vehicle had actually been dispatched o the exception list just kept growing

(I'll stop typing their comments as it just becomes too depressing.)

The estimate is that 20 people are now dead who would otherwise still be alive.

Trevor Jenkins, 134 Frankland Rd, Croxley Green, Rickmansworth, WD3 3AU email: tfj@apusapus.demon.co.uk phone: +44 (0)923 776436

### [Also noted by tjfs@tadtec.co.uk (Tim Steele).]

### 🗡 SPT-4

Hermann Haertig <haertig@gmd.de> Tue, 27 Oct 1992 09:07:36 GMT

The International Conference on Structural Failure, Product Liability and Technical Insurance, held every 3 years in Vienna, was last held in July 1992. This year's conference covered a wide range of topics. An incomplete list:

- failure case studies (e.g. lots of bridges)
- failure analysis using mathematical models and computer simulations (e.g. NW Detroit MD80 crash)
- the influence of computer animation on court decisions
- international liability law
- corrosion
- not much on computer risks though

It turned out to be a real interdisciplinary(engineers of many disciplines + lawyers ) and very international event. Some of the presentations were very professional, e.g. those of lawyers describing the use of computer animation at court.

Proceedings announced to appear in Elsevier later this year.

-- hermann haertig, Project BirliX, GMD (German National Research Center for Computer Science) Hermann.Haertig@gmd.de x400: haertig@zi.gmd.dbp.de

# Information America

<wolit@mhuxd.att.com> Thu, 29 Oct 92 16:49 EST

In the November, 1992, issue of ONLINE, is a horrifying article (pp. 103 - 105) in the "Legal Briefing" department by one Teresa Pritchard-Schoch, entitled, "Information America: A Tool for the Knight in Shining Armor." The author gushes on about what a wonderful boon the Information America database service is for lawyers (her "Knights in Shining Armor") and others. A few extended quotes:

"In one interesting case we (the research staff at a law firm) investigated an entire jury's background before the members were even selected. The case involved three affluent plaintiffs.... Our goal was to find a jury who would not have any sympathy for the plaintiffs.... By checking a motor vehicles license database and real estate property records, we were able to compile a jury whose members all except one drove cars more than six years old. Moreover, no one on the jury owned any real estate. Online sources also revealed facts about the jury members' likes and dislikes which were subtly used to influence them at trial. The opposing counsel was completely unaware of the tactics our firm used and probably still wonders why he lost that case. . . ."

"Information America databases for investigative services include Sleuth, Asset Locator, Executive Affiliation, People Finder, Business Finder, and Litigation Prep.

"Sleuth searches millions of public records from both state and county sources, including corporate and limited partnership records, UCC and lien filings, . . . assumed and fictitious names. . . . The relationships between individuals and business would be almost impossible to duplicate manually. . . ."

"Asset Locator search real property records, aircraft registration . . ., stock holdings . . ., and personal property locators. . . . A real property search for transfers, rather than holdings, is also available. . . ."

"People Finder accesses 111 million names, 92 million households and 61 million telephone numbers. The profile obtained includes the current address, telephone number, residence type, length of residence, gender, date of birth, up to four household members and their dates of birth, and up to ten neighbors and their names and addresses. The sources of information . . . include telephone directories, the U.S. Postal Service's change of address file, direct marketing records, publishers' address files, driver's license files, voter registration records, birth and wedding announcements, etc."

The author acknowledges that "many . . . feel somewhat unsettled" about her accounts, and that "Others are uneasy about increasing availability of private information about their personal lives." But, she argues, "this information has always been available."

I know that commercial credit-reporting firms, such as TRW, must make individuals' files available to them for inspection and correction. Do such laws apply to database services such as Information America as well? Do any states provide individuals with rights concerning the commercial use of personal information identified with them? (In the case of credit services, you usually sign away any privacy rights when you apply for credit, but I wasn't aware that subscribing to a magazine resulted in the same forfeiture.) Are there any other services such as this that provide comprehensive access to a wide range of personal information about private citizens?

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 908 582-2998, wolit@mhuxd.att.com

## // Interesting/obscure interaction between users -- shared mem resources

"David A. Honig" <honig@ruffles.ICS.UCI.EDU> Thu, 29 Oct 92 14:48:05 -0800

I have found that a single user can use up all the shared memory segments that any Sun's kernel allows. (Typically 100 segs of 1MB each,

max). If these are not deallocated correctly, they linger until the machine is rebooted. Talk about "persistent" environments.

### NSF Net cable-cut story is bogus

John G. Scudder <jgs@merit.edu> Thu, 29 Oct 1992 02:31:21 -0500

I noticed the article entitled "The NSF Net cable-cut story" in <u>RISKS-13.86</u>. It clearly looked bogus (9.6k? Come on!), so I asked around a bit. Doug Humphrey had the answer. I have appended his description of the real story below (with his permission).

The RISK here is in believing everything you read...

Regards,

--John Scudder, Merit/NSFNET Internet Engineering jgs@merit.edu

> Date: Wed, 28 Oct 92 18:50:01 -0500

> From: Doug Humphrey <digex@access.digex.com>

> To: jgs@merit.edu

> Subject: [jgs@merit.edu: Re: .0045 mbits/sec]

>

> Concerning the message in RISKS, here is the story; I hope

> that you find it as funny as I did.

>

> A guy from JvNCnet sent out a message about the T3 being cut,

> and mentioning that traffic was being routed over their T1

> connection until the "backhoe fade" was over. Just for fun,

> I modified the message and sent it to a private mailing list.

> The mods that I made were the name of the org (I called if JNvCnet)

> and the speed of the backup feed (I said 9.6k rather than T1)

> and of course I gave it a title of .0045mbits per second.

> I also changed the name of the sender to Steve Martin (a famous> comedy person).

>

> In any case, I sent this to a small, private group of network
> heavies, to whom it would be grand fun. Imagine my surprise
> when people from around the world start forwarding copies of
> RISKS to me with congrats on having such an obvious spoof
> published as fact! Obviously one of them liked it enough
> that he sent it to RISKS.
> In any case, the original sender name is lost to time; I don't
> remember it. It really was a pretty routine message from them,
> ignoring the mods that I made.

> So, that is the story. I hope that helps explain it!

>

> Doug Humphrey, President, Digital Express Group, Inc. doug@digex.com

[Golly, it was neither April Fool's Day nor Two-Backhoe Rode. PGN]

### Ke: Risks in Banking, Translation, etc. (RISKS-13.86)

Arun Welch <welch@cis.ohio-state.edu> Tue, 27 Oct 92 13:01:52 -0500

... indicates that over 75% of bank computer programs are written in a language appropriate to the task as opposed to trying to force their models into the latest Object Oriented fad and 84% of banking software is designed to run on systems that have low mean time between failures

By an amazing coincidence, I've been talking to people at a bank about their current technology, and they are in something of a crisis. This is a large bank that's in the process of taking over smaller banks, and they're currently buying banks at the rate of 3-4 a month, but they're only able to deploy systems at the rate of one every 3-4 months. They're also in a state where most of their software was originally written in the early 70's, and now consists of mostly patches to the original. Their solution? To hop on the OOP bandwagon, and target PC's as the delivery vehicle. Unfortunately, their idea of rapid deployment is instead of taking 5 years to deploy a system to do it in 3, and they're unwilling to give up their ingrained programming structure so they've got 5 people spending six months on a program that took me an hour to prototype. (Not that I'm claiming to be a hot-shot programmer, only that if you put too many people to solve a rather simple problem you're not going to go anywhere) They've got the right idea, but the implementation sucks. It's also interesting to note that the people who will be responsible for accepting whether the new technology works are the people currently running the old technology systems...

welch@cis.ohio-state.edu Arun Welch, Lisp Systems Programmer, Lab for AI Research, Ohio State University

# ✓ Cellular reception equipment banned by Congress

Robert Allen <Robert.Allen@eng.sun.com> Tue, 27 Oct 92 17:56:46 GMT

For some time, since the Electronics Communications Privacy Act was passed, it is been a Federal crime in the U.S. to listen to communications carried out over cellular telephone. Only a handful of people have been prosecuted, mostly cases where someone has taped a politician talking about things (sometimes illegal things) over a cellphone and passed the tape on to the media.

More recently, manufacture and import of devices capable of receiving cellular transmissions have been banned by the FCC. Naturally this has resulted in a run on radios which are 800MHz capable, or which can be easily modified to to be so capable.

The reason the ban on both listening and making equipment capable of listening is that the cellular phone lobby wants to be able to assure their potential customers of privacy. Comments about facist gov't aside, the risks should be obvious: if people assume that a medium is secure, when in fact it is not only NOT secure, but is rather heavily monitored, they are likely to say things they don't mean, or which shouldn't be (literally) broadcast. Currently the police use cellphones extensively, as do drug dealers. Court cases have stated that cordless phones (the type which talk to the base-set in your house) are \*not\* protected under the ECPA, and may be legally monitored, although there is reportedly a law in CA which makes it illegal to do so. In at least one case police have monitored communications on a cordless phone, with a readily available scanner, and have used evidence so gathered to prosecute an individual for drug related crimes.

Another interesting note is that the law specifically prohibits "scanning receivers" which are, or may be made, cellular capable. How this affects test equipment, non scanning receivers, other cellphones, etc., remains to be interpreted by a court.

Here is the partial text of the law.

Robert Allen, rja@sun.com

Article 2202 of alt.radio.scanner: >From: walsh@optilink.UUCP (Mark Walsh) Newsgroups: alt.radio.scanner Subject: Section 408, was "Scanner Bill" Date: 21 Oct 92 17:24:33 GMT

SEC. 408. INTERCEPTION OF CELLULAR COMMUNICATIONS.

(a) AMENDMENT -- Section 302 of the Communications Act of 1934 (47 USC 302) is amended by adding at the end the following new subsection:

"(d)(1) Within 180 days after the date of enactment of this subsection, the Commission shall prescribe and make effective regulations denying equipment authorization (under part 15 if title 47, Code of Federal Regulations, or any other part of that title) any scanning receiver that is capable of --

"(A) receiving transmissions in the frequencies allocated to the domestic cellular radio telecommunications service,

"(B) being readily altered by the user to receive transmissions in such frequencies, or

"(C) being equipped with decoders that convert digital cellular transmissions to analog voice audio.

"(2) Beginning 1 year after the effective date of the regulations adopted pursuant to paragraph (1), no receiver having the capabilities described in subparagraph (A), (B), or (C) of paragraph (1), as such capabilities are defined in such regulations, shall be manufactured in the United States or imported for use in the United States."

Mark Walsh (walsh@optilink) -- UUCP: uunet!optilink!walsh

#### Ke: 15th National Computer Security Conference in <u>RISKS DIGEST 13.87</u>

Dorothy Denning <denning@cs.cosc.georgetown.edu> Tue, 27 Oct 92 08:55:33 EST In response to my earlier message about registering encryption keys, some people have asked how can I be sure that criminals won't use non-registered keys. I don't have a foolproof answer, but consider phone calls. Most people who want to encrypt will buy a commercial product with a built-in key. The key could be registered when the product is bought. Yes there could be a black market in non-compliant products, and the likelihood of that increases every day that we fail to take action on this issue.

Peter Boucher also asked about the benefits of registering keys with a federal agency. After discussing this problem with law enforcement officials and criminologists, I am convinced we are facing a potential crisis in law enforcement if we lose the capability to conduct court authorized taps. The economic value alone of conducting lawful electronic surveillance is estimated in the billions. Much of this is related to organized crime.

Larry Hunter asked how can we be sure that the key centers won't collude with the Department of Justice and give out the key. If the relationship between the phone companies and DOJ is any indication, this won't happen. The folks at the phone companies are so fussy about court orders that they send them back if the semicolons aren't right. And don't forget that even if the key center (which I envisioned as a non-governmental agency) and DOJ collude, they still need to get the bit stream from the phone companies. But if this doesn't satisfy you, Silvio Micali has an even tighter scheme that would allow your private key to be broken up into five piece and shared with 5 trustees. All five pieces would be needed to restore the key, but the pieces could be verified as allowing proper restoration without the need to actually put them together. He calls this "fair public-key cryptosystems."

Dorothy Denning

## Ke: (Denning, <u>RISKS-13.86</u>)

Peter Wayner <pcw@access.digex.com> Tue, 27 Oct 92 16:08:31 -0500

>1) Can you trust the criminals to provide the keys to their data and to use> those keys (and no others) when transmitting incriminating data? If not,> what's the point?

Actually, my favorite solution to this criminal problem is to use a one-time pad. Then it is possible to come up with two keys. One that decrypts the conversation into a benign one and one that decrypts it into the real message.

For instance:

Message: P L U T O N I U M R E A D Y Key # 1: 1 4 10 5 7 8 12 19 4 3 10 19 21 10 Crypttext: Q P E Y V V U N Q U O T Y I Key # 2: 10 24 0 24 2 19 13 25 14 6 3 19 5 4 Message 2: G R E A T C H O C O L A T E

So the criminals send key #1 to their cohorts and register key # 2 with the Federal Key Exchange Registry. When the cops bug the line all they hear about is the stories about their trip to Hershey PA.

Of course non-one-time-pad systems can't work this way. DES can't be rigged this way.

-Peter Wayner

# Ke: (Denning, <u>RISKS-13.86</u>)

<li@oracorp.com> Thu, 29 Oct 92 14:55:51 EST

In <u>Risks-13.87</u> a few people expressed concern that how one could trust a single "independent" agency and whether such an agency exists or could ever be formed. It seems that Prof. Denning's scheme could be easily extended to use threshold schemes (including threshold signature schemes) so that such trust is spread among many (and perhaps mutually hostile) agencies to reduce the chance of corruption and collusion.

Li GONG, ORA Corp., Ithaca, NY 14850

## Ke: 15th National Computer Security Conference (<u>RISKS-13.86</u>)

Carl Ellison <cme@ellisun.sw.stratus.com> 27 Oct 92 21:10:14 GMT

>I believe this scheme is pretty tight. Silvio Micali has evidently invented >another method of safeguarding the keys in a registry, called "fair >cryptography", but I don't know the details. > Dorothy Denning

The scheme is not tight. This assumes that the Executive branch:

1. has a right to eavesdrop on citizens

2. can be trusted not to exceed its authority

If you assume that the government agencies are those of the Nixon Administration -- or worse, those which we would have had if Watergate hadn't been exposed -- you need a much tighter protocol to prevent abuses.

You need to specify the characteristics of the key agency and the key acquisition process so that even if the Executive branch is completely corrupt, the rights of the citizens are protected. You should probably also allow for the possibility of collusion by the Supreme Court, given what we've seen in recent years.

So, how about a protocol in which approval of all three branches of government -- and probably both the house and senate -- hopefully with a majority vote in

each -- is needed for each specific key -- or better yet, for each message in each key? Let those branches cooperate in decrypting the session key for a message and let them deliver the decrypted message (or session key) to the FBI. If that were part of the protocol, then I'd believe that you're getting close to the kind of protection which US citizens deserve.

Of course, the proper solution is an amendment to the Constitution guaranteeing a right to privacy for all citizens -- probably prohibiting all wiretaps, in the process.

I'm told that the State of Alaska has a guaranteed right to privacy.

If that's true, are wiretaps allowed on calls within the state?

Carl Ellison, Stratus Computer Inc, 55 Fairbanks Boulevard ; Marlborough MA 01752-1298 cme@sw.stratus.com (508)460-2783 FAX: (508)624-7488

#### Ke: Denning, <u>RISKS-13.86</u>

Charles Mattair <mattair@sun44.synercom.hounix.org> Tue, 27 Oct 92 09:58:31 CST

Given the attitude of the FBI/NSA/DEA/et al., as to warrantless searches, the ability of NSA to tap most communications without the service providers knowledge and the current circus of everybody investigating everybody WRT Iraqgate, I fear Ms. Denning places a little too much trust in the trustworthiness of the Federal Government.

Incidentally, she appears to overlook the risk after step 3: my key, in plaintext, is available to anybody with access to the paperwork for the triggering investigation. Furthermore, given the propensity of the Federales to engage in "shotgun" type investigations - witness Operation Sun Devil - my crypto security may be compromised for completely fallacious reasons.

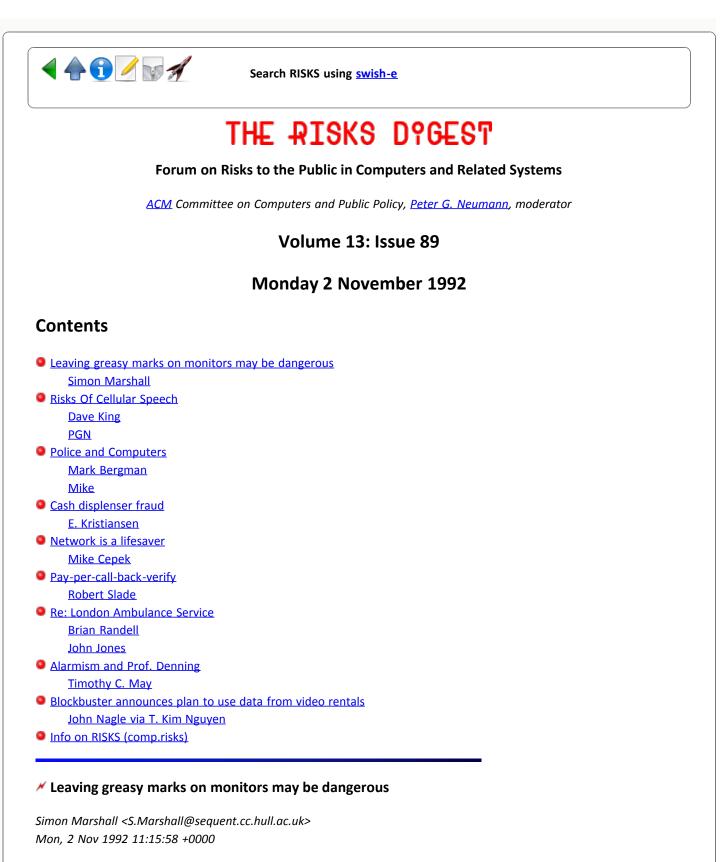
**Charles Mattair** 

mattair@synercom.hounix.org



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Many people regard greasy marks on monitor screens a nuisance. If there is any danger, it is the donor who is at risk because s/he many get some verbal or perhaps (tongue in cheek?) physical abuse from subsequent users. Not so.

This weekend, I cleaned the monitor of a workstation I was using in our lab. Heeding warnings about getting electric shocks from static build ups, I turned the monitor off for a minute before applying the anti-static cleaner. When I began to wipe off the water-based cleaner with a paper towel, the screen burst into flames. Blue-yellow flames may look nice with a beige plastic `dimple effect' surround, but they are not good for the skin.

Apparently, so I am told, CFCs have been replaced in these aerosols by flammable propellants. The risks are clear: the housekeeping maintenance of a computer is not without its dangers. If the lab had a lower ceiling, and I was not able to blow the fire out, this story might have been a different one.

Simon Marshall, Dept. of Computer Science, University of Hull, Hull HU6 7RX, UK Email: S.Marshall@Hull.ac.uk Phone: +44 482 465181 Fax: 466666

#### Kisks Of Cellular Speech

Dave King <71270.450@compuserve.com> 02 Nov 92 12:00:22 EST

[The following was distributed here at work by our security folks. I was surprised at the degree to which cellular traffic has apparently become public speech. But then, perhaps my surprise is just a reflection of my naivete. I'm not sure how Canada's laws compare to ours, but given how difficult it must be to catch someone at this, I can't imagine things are much different here in the 'States. (But then if it's so difficult, how'd they do the study???) Dave]

Two Bell Canada security managers shared some startling data with us recently. In a three-month study of the Metro Toronto area earlier this summer, Bell found that 80 percent of all cellular telephone traffic is monitored by third parties. Even more eye-opening is the fact that 60 percent of monitored calls are taped for closer scrutiny and culling of marketable information. The chance of being monitored and taped is even higher in rural areas, where air traffic is lighter. Scanners cost as little as \$200, and are sold in virtually every shopping mall in Toronto.

Marketable information includes the obvious -- mergers, take-overs, market and product plans, but the listeners are also looking for voice/phonemail access codes and passwords.

The digitized tones are translated into numbers quite easily. "Phone phreaks", the telecommunications equivalent of computer hackers, use these numbers to break into voicemail systems. One misuse which is growing in frequency is the setting up of "pirate" voicemail boxes, often by organized crime. Pirated boxes give them the ability to disseminate information on drug deals, as one example, with little or no risk of detection.

We ask you to be extremely cautious when using your personal or business cellular phone. Do not discuss confidential business matters, and avoid calling in for phonemail messages via your cellular phone.

David L. King, IBM SE Region Information & Telecomm Systems Services Department CAY, Mail Drop D072, 10401 Fernwood Road, Bethesda MD 20817 301 571-4349

#### Cellular Snooping and Privacy Issues

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 2 Nov 92 9:49:24 PST

An article by John Flinn on the front page of the San Francisco Examiner, Sunday, 1 November 1992, listed several cases of inadvertent or advertent eavesdropping, in the midst of a fine story on the problems in general.

- \* A supposedly private conference call among SF Mayor Jordan, real-estate magnate Walter Shorenstein, and several others discussing the then not public withdrawal of George Shinn from the effort to save the SF Giants was BROADCAST on a TV frequency.
- \* "On the first day of the Soviet coup against Mikhail Gorbachev last year, a scanner buff overheard Vice President Dan Quayle making a call from Air Force Two to Sen. John Danforth about the unfolding crisis."
- \* "In New Hampshire, an anti-nuclear activist picked up calls made from the control room at the Seabrook nuclear plant, including one real-life Homer Simpson saying, ``I've got a bad feeling about these valves."
- \* A Green Bay Packer football player was overheard calling a male escort service and making explicit requests.
- \* A 23-minute conversation allegedly between Princess Diana and a man who called her ``my darling Squidge'' was taped by a retired bank manager in Oxford, and transcribed in The Sun. (The woman allegedly referred to the Royal Family as ``this \*\*\*\*ing family''.)

After discussing privacy laws, legalities, and realities, Flinn notes that at Scanners Unlimited in San Carlos, CA, "about a quarter of the customers are interested in telephone eavesdropping."

## Police and Computers

Mark Bergman <bergman@panix.com> Mon, 2 Nov 92 12:14:35 EST

Police Officials Cited for Searching Private Computer Records

LOS ANGELES (AP, 30 Oct 1992) -- More than 45 police officials have been cited since 1989 for using department computers to check the backgrounds of baby sitters, house sitters and others for personal reasons, records show. "It's a very serious problem," Police Commissioner Ann Reiss Lane said. The citations came to light after a civilian Police Commission investigator was suspended 10 days for using department computers without permission to get confidential data on white supremacist Tom Metzger and actor Arnold Schwarzenegger.

The union representing Robert Bauman appealed the suspension and

submitted records showing that more than 45 department employees had been disciplined in the last three years for illegal computer use. Most received suspensions of two or three days or verbal reprimands. As an example, Lane said Thursday, an officer might use the computer to check the background of an individual about to marry one of the officer's relatives.

Bauman's 10-day suspension without pay was upheld last week by the Civil Service Commission. Bauman, a 23-year civilian employee, said he already has served the suspension and was back at work. Bauman, a permit processor, routinely uses police computers to check the criminal records, police files, and tax records of people applying for police permits for massage parlors, gun stores and pawn shops. He said he gathered information on Metzger because he is a part-time historian who does research on right- and left-wing political groups. Bauman said he tapped into Schwarzenegger's files because a co-worker was curious about the actor.

Mark Bergman 718-855-9148 bergman@panix.com {cmcl2,uunet}!panix!bergman

#### Ke: Police misuse computer checks

<"Mike"> Sun, 01 Nov 1992 22:24:51 CST

Other than the obvious RISK, I'd like to point out that much or all of the data in question here is likely kept by government mandate.

On a personal note, I recently recommended to a fellow employee that she report a third employee to her supervisor for a similar thing. #3 had offered to access credit data on someone that #2 was having personal and legal trouble with. What appalled me what that neither one thought there was anything wrong with "using the system" in this way -- until I explained it in terms of \*their\* credit being revealed. <sigh>

## Cash displenser fraud

"E. Kristiansen - WMS" <EKRISTIA@estec.estec.esa.nl> Mon, 2 Nov 92 09:10:43 CET

Several Dutch newspapers recently carried the following story:

The Dutch bank Rabobank has discovered a fraudulent use of their cash dispensers (The term ATM is not commonly used around here. A cash dispenser does just that - dispense cash from your bank account). After you have supplied your card, PIN, etc, banknotes for the desired amount will appear between the "jaws" of the machine. The notes are held rather firmly, and the jaws have a detection device to sense when the money has been removed. If you do not take your money within a given time, the machine will swallow it back, and undo the transaction on your account. The trick is that it appears to be possible to remove part of the stack of notes without the machine noticing. AND THE MACHINE DOES NOT COUNT THE MONEY IT TAKES BACK.

Erling Kristiansen - ESTEC

## Metwork is a lifesaver

"Mike Cepek, MGI" <cepek@vixvax.mgi.com> Sun, 01 Nov 1992 22:25:54 CST

Here is a positive story on the RISKS theme. I have summarized from the page 1A article of the 31-Oct-92 (Mpls, MN) Star Tribune entitled:

After computer note from France, a life is saved

Chris Ginther, a student and computer sales clerk, logged into his home computer Wednesday evening to read his email. One message was from "Emily", a pen-pal of his for several years in Bordeaux, France. The message said she felt cold, alone and empty, that her life was futile. The message said goodbye, and that she was going to kill herself in a few hours.

Across a network he contacted her -- she answered. He got her phone number and called her. Her weak, quiet voice said she wanted to die; that she had taken half a bottle of sleeping pills; that she was alone.

Ginther and an AT&T operator were eventually able to explain the situation to French authorities. An ambulance soon arrived at her house, they smashed the door down, and found her barely breathing. "If we came one minute later," a paramedic said, "she would have been dead."

Ginther has since received messages from Emily as well as her family for his heroic role. Emily regrets her foolish act, and is feeling better about her life now. Fortunately, Ginther doesn't wait until morning to read his email.

## Pay-per-call-back-verify

<rslade@sfu.ca> Mon, 2 Nov 92 11:07:31 PST

Padgett Peterson was telling me about his recent success in getting a BBS set up with one of the new modems with a "caller-id" feature. I think this is going to be a feature that a lot of sysops are going to want.

It happened that just last week I had a request to look into a security problem for a local sysop. He is concerned with security and misuse of his board, and so he has installed a call-back-verify system to check out callers. If he can't call back and get a confirmed phone number, they don't get an account. Many sysops use this to avoid having to "voice verify" each and every caller.

Most call back verify systems have an option that will prevent the system from returning long distance calls. Obviously, this will also apply to "900" pay-per-call numbers. Padgett reminds me that recently there was a scam in New York wherein pager wearers were "paged" by "576" pay-per-minute calls.

The problem in Vancouver is that BC Tel has recently started up pay-per-call

numbers, but they do not yet have identifiable prefixes. Therefore, ankies have been calling various BBSes that have call-back-verify, and leaving these pay-per-call numbers. The sysop who talked to me had lost about \$50 in the last month, and this has only just started.

Vancouver Inst. for Research into User Security, Canada V7K 2G6 604-526-3676 Robert\_Slade@sfu.ca ROBERTS@decus.ca rslade@cue.bc.ca p1@CyberStore.ca

## Ke: London Ambulance Service

<Brian.Randell@newcastle.ac.uk> Fri, 30 Oct 1992 10:54:22 GMT

Despite all the other news, this story is still getting extensive coverage here in the UK. The Independent's follow-up today (30 Oct.) to yesterday's front page story appears as the main story on page 2. It identifies - for the first time as far as I am concerned - the software company involved (Systems Operations - a company I have not heard of before) and adds quite a bit of detail and commentary to the original story, so again I thought it appropriate to submit the complete item (without permission) to RISKS.

Brian Randell

Dept. of Computing Science, The University, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 91 222 7923 FAX = +44 91 222 8232

# SOFTWARE FAILURE "MAY BE BEHIND AMBULANCE CRISIS" By Susan Watts and Ian McKinnon

Computer specialists yesterday said that the system blamed for this week's crisis at the London Ambulance Service appeared to ignore basic tenets for software where breakdown would put lives at risk. The failure of the computer system over 36 hours on Monday and Tuesday, which was said to have cost between 10 and 20 lives, raised serious questions about the way it was designed and tested, experts said. Yesterday, the software company involved, Systems Options, refused to comment.

Leaders of London's ambulance staff last night revealed they had given the services's new chief executive three days to review the efficiency of the computer system. Organisers of the public employees' union, Nupe, said they would have preferred the Computer Aided Dispatch system to have been shut down because it was a danger to the lives of patients.

But Chris Humphreys, the union's London regional organiser, said they had chosen to allow a short period of grace to Mark Gorham, the acting chief executive who replaced John Wilby after his resignation in the wake of an outcry over delays of up to 11 hours in the arrival of emergency vehicles. However, Mr. Hunphreys refused to disclose what action the union planned to take if the management refused to meet its demands or arrive at a satisfactory compromise. He emphasised that by reverting to the system in use prior to full computerisation on Monday and Tuesday, patients' lives were still at risk. Ambulance staff argue that the system of partial computerisation, used in conjunction with radio and telephone to send ambulances to emergency calls, had already led to 45 deaths in the capital because of delays.

However, Mr. Gorham yesterday held out an olive branch when he met union leaders by promising to conduct a full investigation into the 20 deaths ambulance staff said were the result of delays and breakdown earlier in the week.

Robin Bloomfield, a consultant who advised the Government on a programme to promote the safety of computer-controlled systems, said it was a fundamental requirement for this kind of system to have several layers of defence against fialure. He said the ambulance service was asking a lot of its computer system. "With about a million calls a year the system has to be more reliable than a nuclear reactor protection system. I would expect to see a detailed safety case for justifying its operation, and several different back-up systems". He said that as the system originally went into operation, the only back-up it appeared to have was the expectation that people would make their own arrangements if the system failed.

"Safety critical" software should always be passed to an independent assessor to make sure it does what it is supposed to, and passes safety checks. This is standard practice as part of the "safety culture" of companies in the nuclear and transport industries which often use software on which people's lives depend. Such software should have at least one back-up system which could be manual, electronic or even an administrative procedure, ready to switch into operation should something go wrong. Mr. Bloomfield said. "You would very rarely rely on a single system."

Extra calls on Monday exacerbated the situation, but the computer system should have been designed to cope with this. Tom Anderson, a director of the Centre for Software Reliability in Newcastle upon Tyne, said: "If you are getting overload the system should go into a fall-back mode". [...]

More than a quarter of accident and emergency ambulances from the London Ambulance Service are failing to meet performance standards in the Patient's Charter, Tom Sackville, Under-Secretary of State at the Department of Health, said in a written Commons answer yesterday.

The Charter sets a 14-minute response time as the standard for London. Latest statistics, for 1990-91, show 26.3 per cent falling below it, even though in 11 per cent of cases ambulances were able to respond in just seven minutes.

#### Failure of London Ambulance despatch system

John Jones <jgj@cs.hull.ac.uk> Sun, 1 Nov 92 18:05:59 GMT

Today's `Independent on Sunday' (1st November, 1992) has further details relating to the failure of the automatic despatch system introduced by the London Ambulance Service last Monday. While it is difficult to get hard detail from a newspaper article, some of the points made include:

- the despatch system could not distinguish between duplicate

calls relating to the same incident. In some cases several ambulances turned up to respond to the same incident.

 logged calls were lost. One particular case is related in detail, in which a disabled woman was trapped in her chair by the body of her collapsed husband. She called the LAS every 30 minutes, on each subsequent call being told that there was no trace of the earlier call. An ambulance eventually arrived 2.75 hours after the initial call, by which time the husband had died.

The article also relates details of the pathetic attempt by the LAS and government to `manage' the publicity over the failure. When the LAS management eventually pulled the system out, on Tuesday, they initially tried to ``deflect blame onto the staff''. On wednesday, a government minister announced that the `computer had broken down'.

John Jones, Department of Computer Science, University of Hull, UK.

### Alarmism and Prof. Denning

Timothy C. May <tcmay@netcom.com> Mon, 2 Nov 92 09:43:48 -0800

As you know, there has been a huge response to the "key registration" idea. I posted a synopsis of the Dorothy Denning proposal in sci.crypt as "A Trial Balloon to Ban Encryption?" So far, over 200 responses to this "risk." The following piece was posted a few days ago (Friday) to sci.crypt.

--Tim May, 408-688-5409, tcmay@netcom.com

Date: Thu, 29 Oct 1992 23:29:53 GMT Newsgroups: sci.crypt From: tcmay@netcom.com (Timothy C. May) Subject: Alarmism and Prof. Denning Organization: Netcom - Online Communication Services (408 241-9760 guest)

Several people have complained, either in this group or in e-mail to me, that some of my recent comments have been alarmist and detract from what they consider to be my otherwise well-taken points. Fair enough.

In one posting I said "Be afraid. Be \_very\_ afraid." I assumed most folks would recognize this as the tag line from the movie "The Fly." I thought it euphonius, so I borrowed it. In any case, having some fear of what governments may do to us seems to me to be a healthy thing.

I took great care to be as reasonable and as calm as possible a few days ago when I posted the first message in this thread ("A Trial Balloon to Ban Encryption?"). Clearly the key registration idea is controversial.

Now let me be even \_more\_ reasonable. I think Professor Denning has done us a great service, as it has gotten some healthy debate going about these very

important issues. The more than 130 messages, most of them making excellent points, in this group (and a few others, peripherally) indicate the intense interest and scrutiny this subject has attracted.

Dorothy Denning has long been involved in crypto (she wrote the book, so to speak) and more recently in hacker matters, as detailed in Bruce Sterling's new book "The Hacker Crackdown." To assume she is somehow pushing this idea, in the legislative sense, seems unfounded. It seems to me that she thought about some of the serious implications of widespread crypto use, developed some ideas (as Ron Rivest did last summer in an article in "IEEE Spectrum"), and talked about them at the recent Computer Security Conference. Now we may think her particular idea is wrong, for political and technological reasons, but we should not villify her for floating the idea.

I used the term "trial balloon" in perhaps a way I should not have. It may have suggested to some that Prof. Denning, who recently relocated to the Washington, D.C. area, is part of a cabal of crypto advisors who are plotting the next stage of our enslavement. (A smiley) So far as I know--and I hope we'll find out soon enough--there is no proposed legislation along the lines Prof. Denning suggested. I doubt she was acting as an agent for the Feds in floating this idea. Just academic freedom at work.

Furthermore, I favor the open discussion of ideas. I am not one to fear discussing some new idea, or technology, or whatever, for fear it will "give Them ideas" or catalyze a crackdown. In an open society like ours, debate is healthy.

I am happy this issue, which is one of several important crypto policy issues that have been simmering for a long time, has come to prominence. I look forward to seeing the debate here.

(The only thing that worries me is that folks may get so clever, cryptographically speaking, that they patch the flaws in the key registration proposal and thus make it more likely to become law. Let's not lose cite of the fundamental issues surrounding liberty, surveillance, and privacy. But since nearly everyone who has posted so far seems strongly committed to civil liberties, these worries are minimal.)

On with the debate.

Timothy C. May tcmay@netcom.com 408-688-5409 W.A.S.T.E.: Aptos, CA

#### Method Blockbuster announces plan to use data from video rentals

T. Kim Nguyen, kim@watnow.uwaterloo.ca <kim%phaedrus@uunet.UU.NET> Mon, 2 Nov 1992 11:50:30 -0500

[Forwarded to RISKS by T. Kim Nguyen, Systems Design Engineer, Document Imaging Systems, JTS Computer Systems Ltd., Toronto kim@watnow.uwaterloo.ca k.nguyen@ieee.org, kim@jts.com uunet.ca!jts.com!kim]

Newsgroups: comp.privacy,alt.privacy

Date: Wed, 28 Oct 1992 17:05:34 GMT From: nagle@netcom.com (John Nagle) Keywords: Blockbuster video data privacy dossier database Organization: Netcom - Online Communication Services (408 241-9760 guest)

Blockbuster Entertainment Corp. announced plans to used its database of 30 million Blockbuster video club members as part of its marketing push into the music business. Blockbuster is acquiring the 7th largest and 12th largest record chains from Shamrock Holdings, Inc, which will make Blockbuster the 7th largest record retailer by the end of November.

Blockbuster sees many opportunities to cross-market home videos and music. Mr. Steven R. Berrard, vice-chairman of Blockbuster, said that Blockbuster could offer free video rentals to customers who buy music from Blockbuster record stores. This works both ways; he was quoted as saying "If you rent a Disney animated film for your children, I know there might be music that appeals to them. This is a significant plus." He, and Mr. Joseph R. Baczso, speaking to reporters and financial analysts in New York, said one of the company's strengths in music retailing will be its base of 30 million Blockbuster video club members and the data it has on those customers.

Whether or not such use of personal data would be a violation of the Video Rental Privacy Act remains to be seen.

John Nagle (ref: Wall Street Journal, 10/28, p. B6).



Search RISKS using swish-e

Report problems with the web pages to the maintainer