

Search RISKS using swish-e

THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 15

Friday, 29 April 1994

Issue 01 (2 September 1993)

- Is there a roboticist in the house? (Ken Birman)
- Computer Problems Slow Airline Flights Southern U-S (David Fowler)
- AFSS Computer Crash Knocks Out Service for 12 Hours (July 93) (Dave Barrett)
- Risks du jour: malpractice; chemical industry vulnerabilities (Phil Agre)
- Newspaper tide tables (Marc Auslander)
- Software design [C.A.R. Hoare] (Paul Smee)
- Re: Cisco backdoor? (Paul Traina, Al Whaley)
- Easy Access to Video Rental Records (David Jones)
- Answers to phone-related questions (Lauren Weinstein)
- Risks of Discussing RISKS (Dennis D. Steinauer)
- Re: Mars Observer tank testing (Kevin Maguire)
- Conference on Technology Conversion (Gary Chapman)

Issue 02 (3 September 1993)

- BETTER airline/travel-agent computer hide-and-seek (Mark Seecof)
- Lost Canadian crime statistics data (Luis Fernandes)
- Risk of incorrect Daylight Saving conversion (Arthur David Olson)
- The Risk of Discussing "the risks of discussing risks" in RISKS (Jeffrey S. Sorensen)
- The risks of CERT teams vs we all know (Fredrick B. Cohen)
- Potential risk in terminal buffer storage (Robert S. Richardson)
- Electronic documents (Mich Kabay)
- Re: Dorothy Denning and the cost of attack against SKIPJACK (Bill Murray)
- Re: Mars Observer tank testing (Donald Arseneau)
- Re: Dial 1 first (Mark Brader)
- COMPASS '94 CALL FOR PAPERS (John McLean)

Issue 03 (9 September 1993)

- Robot Disarms Man (David Fowler)
- The risks of Naive Users (Amos Shapir)
- The first programming errors (Jon Jacky)
- Offshore Data Havens (John R. Bruni)
- Re: The risks of CERT teams vs we all know (Jeff Schiller, Frederick Roeber)
- Re: Lost Crime Stats (Rodney Boyd)

Into the void at the supermarket (Andrew Klossner)

- Re: What Constitutes an Exhaustive Attack? (A. Padgett Peterson)
- Fixing what's known to be broken (Tom Lane)
- Caller ID Blocking and 911 (Monty Solomon)
- Bank mailing problem (Lauren Weinstein)
- Technology export curbs (Mich Kabay)
- Re: Security holes and risks of software like Sendmail (Marcus J Ranum)
- CfP: 1994 Z User Meeting Announcement (Jonathan Bowen)
- Call for Papers, Decision Science Conference (ACSLHL)

Issue 04 (10 September 1993)

- EuroDigital (Brian Randell)
- Brussels Branch Of BNP Hit By Computer Fraud (jxm)
- Screen savers hide what's running below them (Alan Munn)
- Where should we look for risks? (Steve Talbott)
- Re: Security holes and risks of software ... (Geoffrey H. Cooper, John Carr)
- Re: "Offshore Data Havens" (Fred Baube, Gary Preckshot)
- Re: The risks of Naive Users (Mark Brader)
- Re: More Gripen Griping (Mark Stalzer)

Issue 05 (30 September 1993)

- An oxymoron? (Jim Horning)
- Unfriendly fire (Tim Steele via Jim Thompson)
- RISKS BY FAX (Lauren Weinstein)
- Risks of Flying Toasters? (Jim Griffith)
- Ilvushin Il-114 crash (Urban Fredriksson)
- Cancer Treatment Blunder (Brian Randell)
- RFI from phones (was "EuroDigital") (Mich Kabay)
- Fungible microprocessors (Mich Kabay)
- Re: Security holes and risks of software ... (A. Padgett Peterson, Josh Osborne, John Hascall)
- DCCA-4 Advance Program (Teresa Lunt) [long]

Issue 06 (5 October 1993)

- RISKs of trusting e-mail (Theodore M.P. Lee)
- Stocks and Wands (Paul Dorey)
- Dead for 3 years, but computer kept paying bills (Alan Frisbie)
- Newton Tale of Woe (Steven Sargent via Paul M. Wexelblat)
- RISKS of unverified driving records (Mich Kabay)
- Redundant data (Mich Kabay)
- Conditioning and human interfaces (Robert Dorsett)
- Portable phones and fire detectors (Trevor Kirby)
- Re: Cancer Treatment Blunder (Paul Smee)
- Re: Security holes and risks of software ... (Bob Bosen)
- Bank of America fires employee after reading his e-mail? (David Jones)
- E-mail for denial of services and corruption (Fredrick B. Cohen)
- Software Quality vs Staff Size (Mike Willey)

Issue 07 (6 October 1993)

- ISDN telephone glitch in Hamburg (Klaus Brunnstein)
- Japan: IT Security, JCSEC criteria (Klaus Brunnstein)
- Re: The FBI investigating college pranks (Fredrick B. Cohen)
- Re: Conditioning and human interfaces (Robert Dorsett)

- Re: Answers to the mail problem (Fredrick B. Cohen)
- Trusted portions (Fredrick B. Cohen)
- Think of it as an opportunity, not a problem (A. Padgett Peterson)
- Re: Risks of Unverified Driving Records (Robert J Woodhead, Jim Cook, Rex Black)
- CFP "Ethics" Workshop Cuba Feb.1994 (Klaus Brunnstein)

Issue 08 (7 October 1993)

- Control faults cause train crash (Hank Cohen)
- WSJ report on potential problems with 757/767 Autopilots (PGN)
- Typing error causes stock to fall 20% for `a few moments' (Lorenzo Strigini).
- Epitope suit uses computer bulletin board (Tom Hanrahan)
- Libraries (Phil Agre)
- The Panoptic Sort (Phil Agre)
- "Change" and October 1993 CACM (Jim Huggins)
- Mailing list fun (Mark Brader)
- Virus distributed during college computer sale (Jim Huggins)
- Re: Bank of America fires employee ... (Robert Ellis Smith)
- Re: RISKs of trusting e-mail (Bob Frankston)
- Re: The FBI investigating college pranks (Valdis Kletnieks)
- Separating parts in privileged applications (Yves Royer)
- A reference on Ethics (Peter B Ladkin)
- Re: Cancer Treatment Blunder (David Crooke, Jerry Bakin, PGN)

Issue 09 (8 October 1993)

- Risks of disrupting air traffic control ("Mile High Club") (Richard Marshall via Tom Blinn)
- Sound of the Fury, Part II (Peter Wayner)
- Risks of "security" on Apple Newton (Doug Siebert)
- Re: Control faults cause train crash (Dik T. Winter, Marc Horowitz)
- Re: Conditioning and human interfaces (Nick Rothwell)
- Re: Separating parts in privileged applications (Paul Karger, Steen Hansen, A. Padgett Peterson).
- Re: "Change" and October 1993 CACM (Selden E. Ball, Jr., James K. Huggins)
- Re: Libraries and Imagined Communities (Mark Gonzales)
- Re: Cancer Treatment Blunder (Bob Frankston, Rogier Wolff, Jon Jacky)
- Re: RISKS of unverified driving records (Jim Horning, Jim Hudson)

Issue 10 (8 October 1993)

Wiretap Laws and Procedures (Dorothy Denning) [long]

Issue 11 (11 October 1993)

- Yet another spacecraft vanishes (Landsat 6)
- Auto-response missile system (Brian Kenney, Andrew W. Hagen)
- ITAR issues in PGP & Moby Crypto subpoenas (L. Detweiler)
- Wiretap Laws and Procedures (Mark Day, David HM Spector)
- Risks of using phone bill payment systems (Peter A. Grant)
- Draft Swiss AntiVirus regulation (Klaus Brunnstein)
- Risks of "security" on Apple Newton (Berry Kercheval)
- Re: Disrupting Air Traffic Control (Peter B Ladkin, Peter Wayner)
- Give us all your passwords (Steve VanDevender)
- Politics is private property in the panopticon society (Jeffrey S. Sorensen)
- Re: Control Faults cause train crash (Clive Feather)
- Re: RISKS of unverified driving records (Geoff Kuenning)
- Libel and Liability for incorrect databases (Terry Gerritsen via Sarah Elkins)

- Issue 12 (14 October 1993)
 - Networking on the Network (Phil Agre) [long]
- Issue 13 (14 October 1993)
 - Software safety on UK national news (Jonathan Bowen)
 - Warning labels on medication (Bob Campbell)
 - Corrigenda: RISKs of trusting e-mail (Theodore M.P. Lee)
 - Risk of brain-dead mailers... (Graham Toal)
 - Draft Italian Antivirus Law (Luca Parisi)
 - Collins autopilots have a mind of their own (Peter B Ladkin)
 - Lufthansa in Warsaw (Peter B Ladkin)
 - Lest you think that all is rotten in the state of aviation this week (PBL)
 - Dr. Strangelove (was Re: auto-response missile system) (Barry Brumitt)
 - Re: ITAR issues in PGP & Moby Crypto subpoenas (Dorothy Denning)
 - Privacy (Phil Agre)
 - Mathematics of Markets (Mark Brader)
 - Book on Risk Perception (Anthony E. Siegman)
 - Re: CFP "Ethics" Workshop Cuba Feb.1994 (a.e.mossberg)
 - Re: Cancer Treatment Blunder (Sean Matthews, Bear Giles)
 - New Journal: High Integrity Systems (Russ Abbott)
- Issue 14 (18 October 1993)
 - Cable company shows unorthodox children's TV (John Gray)
 - · Risks of Virtual Reality (John Mainwaring)
 - Re: Wiretap Laws and Procedures (Bob Leigh, Robert Firth)
 - Hubble mirror errata (Henry Spencer)
 - Re: Privacy Risk for Toronto Dominion Bank customers (Dave Parnas)
 - Digital Signatures as ID Numbers (Karl J. Smith)
 - File on Four (Pete Mellor)
 - Australian government to replace DES (Kevin Burfitt)
 - The FAA and HERF (Winn Schwartau) [longish but interesting]
- Issue 15 (19 October 1993)
 - Confirmed reservation ... for non-existent flight (Mathai Joseph)
 - Physical Security of ATM Password (Jeff Schultz)
 - Re: RISKs of trusting e-mail (Lars-Henrik Eriksson, Frederick M Avolio)
 - Re: Porn, Wiretapping, DES, HERF (Phil Karn)
 - Re: The FAA and HERF (Ted Wong, Jack Boatman)
 - Re: Digital Signatures (Robert J Woodhead)
 - Re: Risks of Virtual Reality (Robert Carolina)
 - Re: Wiretap Laws and Procedures (Steve Bellovin)
 - Re: Australian government to replace DES (Steve Bellovin)
 - Re: Software safety on UK national news (Pete Mellor)
 - Re: Libraries and Imagined Communities (Bruce Hamilton)
 - Re: Separating parts in privileged applications (Bob Frankston, Tom Thomson)
- Issue 16 (19 October 1993)
 - Social Psychology & INFOSEC (Mich Kabay)
- Issue 17 (21 October 1993)

- A chip, off the old block (PGN)
- Fiber Optic Cable "Meltdown" in Connecticut (E.M. Culver)
- NII confidential report "on sale" (Martyn Thomas)
- US Has It Too (Re: Russian Doomsday Device) (Li Gong)
- Media Explosion => Loss of Community ? (Fred Baube)
- Re: Auto rentals, law suits, and the risks (Jerry Leichter)
- Dangers of anonymous remailers [Anonymous]
- Privacy Digests (PGN)
- SunOS and Solaris vulnerabilities (PGN, CERT Advisory)

Issue 18 (27 October 1993)

- Saab Story: Cars rolling off the assembly line (Vernon L. Chi)
- Yet another date overflow bug (David Lamb)
- OZDISK Big Brother Down Under? (Mike Bell)
- Russian Hacker Activity (David Fowler)
- Thank you (Lauren Wiener)
- Re: CERT and "security incident" handling (Doug Moran, A. Padgett Peterson, Scott Schwartz, Bruce R. Lewis, Nick Rothwell)
- Re: The FAA discovers HERF (Dennis Chamberlin)

Issue 19 (27 October 1993)

- Optic fibre fragment kills Telecom worker (Robin Kenny)
- Lanocaine (sp?) (Bob Frankston)
- Ethernet addresses as "port" ids (Bob Rahe)
- File on Four on safety-critical software (Pete Mellor)
- Cracking feature in the small press (Jim Haynes)
- Re: FAA and HERF a pun-ctilio (Peter B Ladkin)
- Re: Clipper (Fredrick B. Cohen)
- Re: Chip thefts (Mich Kabay)
- Re: Dangers of Anonymous Mailers (Steven S. Davis)
- Re: Swiss AntiViral legislation (Claudio G. Frigerio via Klaus Brunnstein)
- Computer-Aided Verification (CAV'94) (David Dill)

Issue 20 (1 November 1993)

- Breakdown in computerised voter support, Oslo (Reidar Conradi)
- Norwegian hackers fined (\ystein Gulbrandsen)
- White House distributes STONED 3 virus (Andrew Klossner)
- Police feedback (Graeme Jones)
- Taurus Project (E. Kelly)
- Magnetic Fields in Subway Cars (Bob Drzyzgula)
- Report on Software Product Liability (Charles Youman)
- Re: Dangers of Fibre Optic cable (John Gray)
- Re: CERT Reports and system breakins (Mike Raffety)
- Re: CERT (was "security incident handling") (A. Padgett Peterson)
- Re: Ethernet addresses as "port" ids (A. Padgett Peterson)
- 3rd SEI Conference on Software Risk, 5-7 April 1994, Pittsburgh (Ellen Ayoob)
- Workshop on IT Assurance and Trustworthiness (Marshall D. Abrams)
- ISOC Symposium on Network and Distributed System Security (Danny Nessett)

Issue 21 (2 November 1993)

- Investment program turns into doomsday machine (Meine van der Meulen)
- Direct E-Mail: J.S. McBride & Co. (anonymous)

- "RSI does not exist" (Gavin Matthews)
- Public relations (Phil Agre)
- Procrustus (Bob Frankston)
- Re: Magnetic Fields in Subway Cars (Peter Debenham, Andrew Marchant-Shapiro)
- Re: Fiber Optic Cable Hazards (Bonnie J Johnson)
- Re: Breakdown in computerised voter support, Oslo (H?vard Hegna)
- Re: Ethernet addresses as port ids (Bob Rahe)
- ESORICS 94: Call for Papers (Yves Deswarte)

Issue 22 (8 November 1993)

- <u>Direct Subscribers: Can you instead read RISKS as a newsgroup? (RISKS)</u>
- Prague computer crime (Mich Kabay)
- Phiber Optik, Master of Disaster, sentenced (Mich Kabay)
- Mass. state police confuse car owners with gun carriers (Brian Hawthorne)
- Overenthusiastic automated investment programs (John R Levine)
- RISKS of unaccountable computerized elections (Dave Hart)
- Re: Safety-critical software (David Parnas)
- Re: InterNet Mailing List (JS McBride [2])
- Security of the internet (Bill Murray, PGN)
- Yu, "Automated Proofs of Object Code..." available (Jim Horning)
- "Research Directions in Database Security" ed. by Teresa Lunt (Rob Slade)
- Re: CERT Reports and system breakins (Phil Karn, A. Padgett Peterson)
- Call for Participation, FIRST Incident Response Tools Working Group (Michael S. Hines)

Issue 23 (6 November 1993)

- Another plane lands on the taxiway (Lord Wodehouse)
- Pax Technologica? Not in Somalia (Peter Wayner)
- Teachers Beware! (Peter G Spera)
- Clerk stole from ATMs he was told to top up ... (Apte Kishor Hanamant)
- Notice of Fire Hazard with Dell Notebook Computers (Bob Robillard)
- "Eve of the Storm" (*another* Desert Storm virus?) (Rob Slade)
- Re: White House and STONED 3 virus (Andrew Klossner, Jon Grantham)
- Re: Ethernet addresses as "port" ids (Brian Bulkowski)
- Re: CERT Reports and system breakins (Allan Duncan)
- Re: Fiber Optic Cable Hazards (Gordon Mitchell)
- Re: "RSI does not exist" (Pete Mellor)
- Re: Magnetic Fields in Subway Cars (Bob Frankston, Kenneth R Foster, Ian Turton, Peter Gorny, Bruce Limber, Russ Cage, Graeme Thomas)

Issue 24 (9 November 1993)

- Smart Houses? No Thanks! (Jim Brown)
- Ada, a standard no more? (Luis Fernandes)
- Pets & data communication (Bruce Clement)
- Orange County DACS outage (Matt Holdrege)
- Review of Bruce Sterling's Hacker Crackdown (Peter B Ladkin)
- Alvin and Heidi Toffler's War and Anti-War (Jeffrey D. Young)
- Re: Car owners confused with gun owners (Martin Minow)
- Software control problems in Block 40 F-16s (Peter B Ladkin)
- Investment program turns into doomsday machine (Rogier Wolff)
- Re: Notice of Fire Hazard with Dell Notebook Computers (Don Porges)
- Internet Security (William Hugh Murray)
- Stupid language games (Richard Schroeppel)

- Networking on the Network (Richard Schroeppel)
- Anonymous postings (anonymous? No, Daniel Lieber)
- Properties of Anonymizing Service (Anthony E. Siegman)
- Risk-happy drivers foil anti-lock brakes (Dyane Bruce)

Issue 25 (10 November 1993)

- RISKS of camping... (E.M. Culver)
- No change in Ada policy (Robert I. Eachus)
- Groundhog Day, D-Day, Remembrance Day, and all that (Mark Brader)
- Not so easy to be anonymous (Robert L Ullmann)
- Snakes of Medusa and Cyberspace: Internet identity subversion (L. Detweiler)

Issue 26 (13 November 1993)

- Gripen crash report (Urban Fredriksson)
- SAS MD-81 crash report, December 1991 (Martyn Thomas)
- MASS state police confuse car owners with gun carriers (NOT) (Simson Garfinkel)
- Re: No change in Ada policy (Anonymous, Parnas)
- Risk-happy drivers foil anti-lock brakes (Mark Brader)
- Naissance d'un virus soon to be published (Jean-Bernard Condat)
- Re: pseudospoofing (Andrew Marchant-Shapiro)
- I'm Me (Nick Szabo)
- Re: anonymizing service (Karl Lui Barrus)
- Re: Not so easy to be anonymous (Seth Chazanoff)
- Re: Stupid language games (Dave Parnas)
- Re: Networking (Phil Agre)
- "Friendly Fire" in system design (Steve Taylor)
- Re: Teachers Beware! (Andy Cunningham)
- FBI Operation "Root Canal" Documents Revealed (Dave Banisar)

Issue 27 (17 November 1993)

• Re: The Snakes of Medusa and Cyberspace (mathew, Alex Glockner, Perry E. Metzger, Jamie Dinkelacker, Arthur Abraham, Peter Leppik, Brad Hicks, Neil McKellar, Leonard Mignerey, L. Detweiler)

Issue 28 (17 November 1993)

- Power problems stops Milano Stock Exchange for 4 hours (Lorenzo Strigini)
- Lawyer discovers the RISK of computer efficiency (Martin Minow)
- Living Will Database (Brian Hawthorne)
- Review of "Second Contact" by Resnick (Rob Slade)
- UK government to scrap safety laws (Jonathan Bowen)
- Tablespoons, or, handwriting recognition may be hazardous to your poem (Mark Brader)
- Visa introduces transaction UIDs (Bob Frankston)
- Re: CERT Reports and system breakins (Steve Bellovin)
- Re: MASS state police confusion (Eric N. Florack)
- Re: Ada Usage (Harry Erwin, James H. Haynes)
- Re: Groundhog Day, D-Day, Remembrance Day, and all that (mathew)
- A Myth is as good as a Smile (PGN)
- Call-for-Papers for 17th Nat'l Computer Security Conference (Louise Reiner)

Issue 29 (23 November 1993)

- Logic Bomb planted in retribution for nonpayment (Mich Kabay)
- Brazilian computer snarls in corruption probe (Mich Kabay)

Digitized Photos (Mich Kabay)

- Magnetic Fields & Leukaemia (Mich Kabay)
- Who owns the unused cycles? (Bear Giles)
- Not-voting-by-phone Boulder over (Bear Giles)
- Tablespoons, or another risk? (Steve VanDevender)
- Charge cards from mail order houses (Ted Wobber)
- United Parcel Service signatures (Jim Carroll)
- Re: Massachusetts state police confusion (Brian Hawthorne)
- Re: Ada Usage (Douglas W. Jones, Robert I. Eachus)
- Re: UK government to scrap safety laws (Keith Lockstone)

Issue 30 (1 December 1993)

- Risks of automated betting (Russ Corfman)
- Computer Changeover May Cost \$16M (Lin Zucconi)
- Mercury passwords can be compromised (Keith Lockstone)
- Computerized Pornography (Brian Randell)
- Picking from Trash (Re: Charge cards from mail-order houses) (Li Gong)
- GRE goes "adaptive" (Cris Pedregal Martin)
- More news on the Lufthansa A320 accident in Warsaw (Peter B Ladkin)
- Memory error corrupts file (James Michael Chacon)
- New Moderator for the Computer Privacy Digest (Dennis G. Rears)
- Re: Safety-critical software (Pete Mellor)
- Re: Ada Usage (Tucker Taft, Mathew Lodge)

Issue 31 (3 December 1993)

- London Underground train departs driverless with 150 passengers (Martyn Thomas)
- · Voting by Fax (Bear Giles)
- Computer Fax Problems (Andrew Blyth)
- A study of National Cryptography Policy (Marjory Blumenthal)
- "Using McAfee Associates Software for Safe Computing" by Jacobson (Rob Slade)
- New Docs Reveal NSA Role in Digital Telephony Proposal (Dave Banisar)
- Re: Computerized Pornography (Charlie Stross)
- Re: Lufthansa Airbus Warsaw Crash 14 Sep 93 (Udo Voges)
- Re: Mercury passwords can be compromised (Peter Debenham)
- Re: United Parcel Service signatures (Andrew Marc Greene)
- CFP: 13th Symp. on Reliable Distributed Systems (Rick Schlichting)

Issue 32 (7 December 1993)

- FAX sends instead of receives (John McKay)
- Risks of conference calls "lack of announcement"
- Apple Computer Distributes a CD-ROM with a "Trojan Horse" (Saul Tannenbaum)
- French Wiretaps (Mich Kabay)
- Tokyo bank fraud (Mich Kabay)
- German Radicals use Computers (Mich Kabay)
- NJ credit thefts (Mich Kabay)
- Counterfeits (Mich Kabay)
- AIDS data stolen in Florida (Mich Kabay)
- Unauthorized changes of address (George Zmijewski)
- Massive credit card fraud (Mich Kabay)
- Lufthansa Warsaw crash A Clarification (Peter B Ladkin)
- Reminder for DCCA-4: Fourth IFIP Working Conference (Flaviu Cristian)

Issue 33 (7 December 1993)

- Review: "Digital Woes" by Lauren Ruth Wiener (Pete Mellor)
- Review: "Terminal Compromise" by Winn Schwartau (Rob Slade)

Issue 34 (13 December 1993)

- Computer glitch postpones 'Tommy' (David Tarabar)
- Electronic Money (Brian Randell)
- Financial Newswire Fraud (Thomas J Scoville)
- Canadian study on computer fraud (Mich Kabay)
- · Risks of being a programmer (Jon Jacky)
- The risk of distributed servers with only partial uninterruptible power (Bob Cunningham)
- Risks of inband communication triggering call forwarding (Simson L. Garfinkel)
- Mail forwarding as easy as Call forwarding (Kiser)
- Re: Massive credit card fraud (Pete Mellor)
- Apple has poked around on your hard disk before (Grady Ward)
- Re: Corrupted Polling (Brian Randell)
- Re: Digital Woes (Harry Erwin)
- COMPASS '94 Call for Papers and Call for Tutorials (John Marciniak)

Issue 35 (22 December 1993)

- Airport lessons for InfoSec (Mich Kabay)
- Sham CD-ROMs (Mich Kabay)
- Smart Cars and Highways (Mich Kabay)
- Risky Demo Offer (Rex Wheeler)
- "Re-Chipping" Stolen Mobile Phones (Brian Randell)
- Interactive TV: electronic democracy, risks to privacy, etc. (John Gray)
- Trouble with funny place names (Mark Brader)
- Mexico Turns Off Quake Warning System (Frank Carey)
- Wireless Laptop Eavesdropping (Andrew Duane)
- Re: Harry Erwin on Digital Woes (Lauren Wiener)
- Question About Singapore Lottery Crime (Sanford Sherizen)
- ISOC Symposium on Network and Distributed System Security (Dan Nessett)

Issue 36 (2 January 1994)

- Risks of high pitched tones (Lance J. Hoffman)
- Can SETI signals bear viruses? (Brandon A Cantillo)
- Report on Strasbourg A320 Crash emphasises HCI (Peter B Ladkin)
- Be careful not to let your engine control computers overheat (Peter B Ladkin)
- LapLink Wireless (Mark Eppley via Bob Frankston)
- Re: Airport lessons for InfoSec (Robert Dorsett)
- Re: "Re-Chipping" Stolen Mobile Phones (Andrew Beattie, Li Gong)
- An Exception (Harry Erwin)

Issue 37 (3 January 1994)

- Hacker nurse makes unauthorised changes to prescriptions (John Jones)
- Customs Data Diddling (Mich Kabay)
- Credit cards again (Mich Kabay)
- Tax Frauds (Mich Kabay)
- Re: Can SETI signals bear viruses? (Robert Ayers, Dave Weingart, James Abendschan).
- "When H.A.R.L.I.E. Was One" by Gerrold (Rob Slade)
- Request for help with RISKy situation (Alan Wexelblat)

Issue 38 (15 January 1994)

- \$500k phone fraud (Chuck Weinstock)
- Wild agents in Telescript? (Phil Agre)
- "Industry Defies Clinton on Data Encryption" -- John Markoff
- Encryption Export Control, and Cantwell Bill (Sharon Webb)
- (Mis)Information spreads like wildfire (Mabry Tyson)
- Software Management Risks (Harry Erwin)

Issue 39 (21 January 1994)

- Hidden risks of earthquakes (Clive D.W. Feather)
- Phony air traffic controller (Fernando Pereira)
- Poulson/PacBell (Mich Kabay)
- Links to Internet to be limited by DoD (Bob Kolacki)
- India Software Glitch Causes PSLV Failure (S. Ramani)
- Verify your backups (Louis Todd Heberlein)
- Safety in Telescript (Luis Valente)
- Slippery Folks in the Oil Business (Peter Wayner)
- Risks of Domain Names (Matt Cohen)
- Re: Mail forwarding as easy as Call forwarding (John M. Sulak)
- Cellular phone security features...NOT! (Matthew Goldman)
- Harvard Case of Stolen Fax Messages (Sanford Sherizen)
- Re: Hacker nurse makes unauthorised changes to prescriptions (Li Gong)
- Spontaneous recovery from "NOMAIL" setting? (Ron Ragsdale)
- Re: Proposal for new newsgroup on safety-critical systems (Jonathan Moffett)
- Privacy Digests (Peter G. Neumann)
- ISSA Conference Announcement (Dave Lenef)

Issue 40 (24 January 1994)

- Re: Spoofing Air Traffic Control (John Stanley, Wolper)
- Re: Spoofing Telescript (Barry Margolin, Adrian Howard, Paul Barton-Davis, Geoffrey Speare, John Pettitt)
- Re: Spoofing SETI (Someone at NASA?, Bear Giles, Mark Staltzer, Steven King, Steve Elias, Charles Bryant, David Honig, Mark Thorson, Jon Mauney, Andrew Klossner, Dan Keith, Adam BJ Quantrill)

Issue 41 (26 January 1994)

- Lightning on the Ethernet (eddy, not flo)
- E-Mail Fraud (Lori Carrig)
- Update on voter fraud in Costella County, Colorado (Bear Giles)
- Laptop Computer Could Explode (F. Barry Mulligan)
- Opening of European borders delayed by InfoSys problems (Bertrand Meyer)
- Canada loses satellites -- anyone have more info? (Alan Wexelblat)
- Risks of dynamic binding (Andrew Shapiro)
- New museum on cryptography (Jeremy Epstein)
- Is Global Authentication Impossible? (Li Gong)
- Re: Phony air traffic controller (Mark A. Bowers, Cameron Strom)
- Re: Smart Cars and Highways (Jerry Leichter)
- Re: Telescript risks (Bob Blakley III)
- Re: Can SETI signals bear viruses? (Andrew Klossner)

Issue 42 (28 January 1994)

CFP '94: THE FOURTH CONFERENCE ON COMPUTERS, FREEDOM AND PRIVACY [long]

Issue 43 (29 January 1994 [misdated 30 Jan])

- Where has your Floating Point floated to? (Dave Wortman)
- Canadian TeleSat Anik E-2 Down (Colin Perkel, Luis Fernandes)
- Re: Lightning on the Ethernet (Jon Peatfield)
- Re: Spontaneous recovery from "NOMAIL" setting (Al Stangenberger, Ron Ragsdale, Peter M. Weiss)
- Re: Verify your backups (Rob Horn, Dick Hamlet)
- Crypto policy report available online (Lance J. Hoffman)
- 1994 IEEE Symposium on Research in Security and Privacy (Catherine Meadows)

Issue 44 (2 February 1994)

- Canada to monitor phone calls, fax, etc.? (Walter C. Daugherity)
- Risks of cliche collisions on the information superhighway (Phil Agre)
- Irrational risk research (Phil Agre)
- Czech computer fraud (Mich Kabay)
- Clipper Petition (Dave Banisar)
- "Digital Woes" by Lauren Wiener (Rob Slade)

Issue 45 (8 February 1994)

- A Rise in Internet Break-ins Sets off a Security Alarm (NYT excerpt)
- CERT Advisory Ongoing Network Monitoring Attacks (CERT)
- "Misunderstanding" a CERT advisory (Klaus Brunnstein)

Issue 46 (8 February 1994)

- Medical privacy violation (Mich Kabay)
- Revised Documents on FTP server without version number (David W. Crawford)
- Campaign Against Clipper (Dave Banisar)
- · Re: Clipper Petition (David Gursky)
- Don't trust the phone company (Tom Bodine)
- Modern discussion of computer risks in old book (Lauren Wiener)
- RISKs of network surveys (Craig DeForest)
- National Cryptology Museum (Larry Hunter)
- 10th ACSAC Call for Papers (Vince Reed)

Issue 47 (9 February 1994)

- "Sounding the Alarm: Noisy medical alert systems" (B Fitler)
- (Semi-)electronic locks (Pete Kaiser)
- Safety in Telescript, Part Deux (Luis Valente)
- Risks of email exacerbating typos (M. Hedlund)
- Patents Hearing as it relates to Software (Paul Robinson)
- Network surveys et al. (Steve Holzworth)
- Re: Don't Trust The Phone Company (Lars Poulsen)
- Re: "Misunderstanding" a CERT advisory (D.R. Newman)
- Re: Clipper Petition (Pete Kaiser, John Mainwaring)
- Re: Altered White House Documents (Robert Firth, Larry Nathanson)
- EFF Wants You (to add your voice to the crypto fight!) (Stanton McCandlish)

Issue 48 (9 February 1994)

- Notes on key escrow meeting with NSA (Matt Blaze)
- Re: Campaign and Petition Against Clipper (Dorothy Denning)
- Issue 49 (10 February 1994)

- FireFly in the ointment? (Don Watts)
- Aging software ages suddenly! (Don Watts)
- Clinical diagnosticians and diagnostic clinicians (David Honig)
- UK bank preparing for electronic money trial (John Gray)
- What goes around, comes around (Paul Robinson)
- Electronic rumours (Mich Kabay)
- Medicare Transaction System & the Electronic Superhighway (Mich Kabay)
- Re: Risks of cliche collisions on the information superhighway (Mark Jackson)
- Re: White House documents (Bill Casti via David Crawford)
- Re: Cantwell and Spoofed Representatives? (Jon Leech)
- Re: Sounding the Alarm (Robert J Horn)
- Re: Verify your backups (Timothy Miller, Dan Lanciani, Martin Minow)
- EMI article in IEEE Spectrum (Robert J Horn)

Issue 50 (10 February 1994)

 Re: Dorothy Denning's contribution to RISKS-15.48 on EES/Clipper/etc. (Barbara Simons, Marc Rotenberg, George T. Talbot, Lance J. Hoffman, Fredrick B. Cohen, A. Padgett Peterson, Geoff Kuenning)

Issue 51 (10 February 1994)

- FLASH: Vice President Gore Questions Current Key Escrow Policy! (Stanton McCandlish)
- CMU elections suspended due to computer problems (Declan B. McCullagh)
- TCAS blamed for near collision over Portland (Lauren Wiener)
- Pacific Bell Customers Get Unpleasant Messages (Lin Zucconi)
- Two recent UK tales: Gas payment notices; info network problem (Peter Ladkin)
- FBI falsely obtained wiretap in KC (Paul)
- Re: "Misunderstanding" a CERT advisory (Espen Andersen)
- Re: Altered White House Docs (A. Padgett Peterson, Pete Mellor, Jim Hoover)
- About Computer Software and Patents (Paul Robinson)

Issue 52 (11 February 1994)

- Cygnus Support frees its security software to beat Internet break-ins (John Gilmore)
- Re: Campaign and Petition Against Clipper (Dorothy Denning, Marcus J. Ranum, Carl Ellison, Paul R. Coen)
- Re: Notes on key escrow meeting with NSA (Roy M. Silvernail)
- Re: Coincidences (Sniffers, Breakins, and EES) (A. Padgett Peterson)
- Re: Verify your backups (Li Gong)
- Re: Electronic Keys vs. The Old Kind (Morgan Price)
- New List on Computer/Telephone Problems/Bugs/Viruses/Dangers (Paul Robinson)

Issue 53 (12 February 1994)

- Electronic tax filing: MAKE.MONEY.FAST ??? (Ed Ravin)
- <u>Celebrity Risks -- Bill Gates (Jack B. Rochester)</u>
- Computers and Health (Computer User Family)
- Microsoft Software Development Network registration (James Briggs)
- Re: FireFly in the Ointment (Andy Kostic, Marco Barbarisi)
- Re: Sounding the Alarm (Anthony E. Siegman, Georg Feil)
- Re: Don't trust the phone company (Joe Konstan, Spencer W. Thomas, Michal.Jankowski, Nancy Griffeth and others)

Issue 54 (14 February 1994)

- Voice-mail phreaking (Mich Kabay)
- Electronic Food Stamps (Mich Kabay)

- Another ATM "front end" fraud this time caught (Jonathan Haruni)
- [Lighter Side] Risks of computer-literate babies (Robert J Woodhead)
- New Novel/Thought experiment... (Peter Wayner)
- Recent Articles of Interest (Bob Frankston)
- Re: Celebrity Risks -- Bill Gates (John Bush)
- Card Fraud and Computer Evidence (Ross Anderson)

Issue 55 (15 February 1994)

- YAMIC [Yet Another Mistaken Identity Case] (Robert Herndon)
- William Safire on Clipper: ESSAY: SINK THE CLIPPER CHIP
- Over 10,000 Sign Petition to Oppose Clipper (Dave Banisar)
- Canada to monitor phone calls, fax, etc.? (Sahel Alleyasin)
- No switch on new Sun Microphone (Olin Sibert)
- Electronic Mail vs Paper Mail (mathew)
- FIRP report comments (Stephen D Crocker)

Issue 56 (17 February 1994)

- Smart Cards for London Buses (Mich Kabay)
- NII Testimony (Robert Ellis Smith)
- Losing ATM transactions (N.S. Youngman)
- Telephone charges fail to fit the bill (Marcus Marr)
- Re: E-mail risks (Bill Fitler, Rex Black)
- 737 crash near Panama (Tim Steele)
- Re: YAMIC [Yet Another Mistaken Identity Case] (Jim Cook)
- Who says the Clipper issue is complicated? (D.J. Bernstein)
- Re: Classified justifications: escrowed keys (Carl Ellison)
- CFP, First Smart-Card Research & Advanced Application Conference (JJVandewalle)

Issue 57 (22 February 1994)

- Extra line in Chemical Bank program doubles ATM withdrawals (John Sullivan)
- What else happens when the airbag in your car detonates? (William Caloccia)
- SimHealth (Mike Zehr)
- Risks of "doing it right" (David Wittenberg)
- The ultimate couch potato (Bruce Balden)
- Telephone Card Audit Trails (F.Baube[tm])
- E-Mail Courtesy (Dan Yurman, Peter Cherna, Greg J B)
- E-mail to Bill (Aaron Barnhart)
- CompuServe Offers Credit Info (John Murray)
- Electronic Food Stamps (LoQuan Seh)
- Re: YAMIC [Yet Another Mistaken Identity Case] (Bryan J Dawson)
- John Perry Barlow WiReD article on Clipper (Martin Minow)

Issue 58 (23 February 1994)

- E-Mail blunder at Olympics (David G. Novick)
- Dog Gets Card With \$10G Limit (marc via PGN)
- Computer error adds to ad valorem tax for 300,000 people (James E. Burns)
- Embezzler caught by computer trail (James E. Burns)
- Software testing at Sizewell (Brad Dolan)
- Clipping Clinton and the Executive Branch... (Peter Wayner)
- Clipper: Love your country, don't trust its government (David Honig)
- Re: CompuServe Offers Credit Info (Steve Bellovin)
- Social RISKS of Universal IDs (John Oram)

- Re: SimHealth (Gerd Meissner, Bob Frankston)
- Re: Telephone Card Audit Trails (Jonathan I. Kamens)
- Re: E-Mail Courtesy (Jim Haynes, Bob Frankston)
- Re: Electronic Food Stamps (Colby Kraybill)
- Re: International Internet Association (Jeff Porten)

Issue 59 (26 February 1994)

- Microsoft Dinged for \$120 Million
- Leaving intelligence to the experts: lie detectors and Clipper (John M. Sullivan)
- Janitor interrupts UPS (Lisa Balbes)
- Portuguese drug ring ensnared by pager technology (Fernando Pereira)
- Snag hits Reserve Bank of India's clearing operations (S. Ramani)
- "Wire Pirates" article in March 1994 Scientific American (Martin Minow)
- Van Eck Radiation Helps Catch Spies (Winn Schwartau)
- Re: Software testing at Sizewell (Dave Parnas)
- Re: SimHealth (Bill Stewart)
- Re: The ultimate couch potato (Bear Giles)
- FLASH: FBI's Draft Digital Telephony Bill: EFF Summary and Analysis (Daniel J. Weitzner)

Issue 60 (28 February 1994)

- \$1M deposited in bank error (PGN)
- Another Olympic E-mail Penetration (PGN)
- The dangers of electronic mail (Rob Hasker)
- Ex-employee arrested in computer-file theft (Lance Gatrell)
- How about bounties for inspecting safety-critical software? (Michael Chastain)
- Reloadable and Smart Cards en route to worldwide acceptance (Gordon Webster and Sree Kumar)
- FBI Digital Telephony Proposal and PCS mobile phone networks (M. Hedlund)
- Re: Van Eck Radiation ... (James H. Haynes, Fredrick B. Cohen, Vadim Antonov, Bob Brown, John R Levine, Bill Bolosky)

Issue 61 (3 March 1994)

- More on the \$1M deposited in bank error (Raju Varghese)
- Internet Trojans (Mich Kabay)
- Biometrics (Paul Robinson)
- Re: Aldrich Ames and the Clipper Project... (Peter Wayner)
- Some Thoughts on Clipper, NSA, and one key-escrow alternative (Jim Bidzos)
- Algorithms have unclear boundaries (Mike Crawford)
- Response from Cambridgeshire Constabulary (Lawrence Kestenbaum)
- Re: Threatening E-mail (Peter B Ladkin)
- Re: Bounties for Safety-Critical Software (Peter B Ladkin)

Issue 62 (3 March 1994)

- Joe Camel's 10,000,000 best friends (Phil Agre)
- Double Posting of Credit Card Charges (Bryan Apple)
- Video Tech & Privacy... what's becoming possible (David Honig)
- RISK of computer-controlled landings (Simson L. Garfinkel)
- Headline: "Child molesters use computer talk as bait" (David Tarabar)
- Conviction for spreading virus? (Laurel Kristick)
- We {Will} Find you...' (Paul Robinson)
- Local TV News Report Misses The Boat (Dan Danknick)
- Educating on the RISKS of the Internet (Jeremy Epstein)
- Will they ever learn? [Passwords] (Roger Binns)

- One time Passwords and Encryption (A. Padgett Peterson)
- Of Locks and Legends (Dave Pierson)
- Impact fuel cutoff anecdote, risk (Bob Wise)
- NTIA Releases Notice of Inquiry on Privacy Issues (Beth Givens)
- SIGSOFT 94 Call For Papers (Dave Wile)

Issue 63 (7 March 1994)

- Yet Another Mistaken Identity (Mike Zehr)
- Philadelphia 911 Crash (Steve Pielocik)
- Service a computer, go to jail (Kriss A. Hougland)
- Court Case casts doubt on cashpoint credibility (Brian Randell)
- <u>'Hacker' alters Drug Protocol in British Hospital (Peter B Ladkin)</u>
- Will Australia be doomed to repeat Clipper? (Rhys Weatherley)
- A Well Oiled Mac (Jon Golob)
- SCIENCE article critical of computer models (Jon Jacky)
- Re: Autopilot landings in 'zero visibility' (Peter B Ladkin)
- The risks of user ID's (Jason Haines)
- RISKS RISKS: Bug in mailing RISKS-15.61 (Mike Sullivan, PGN)

Issue 64 (10 March 1994)

- Irony & embarrassment (Gene Spafford)
- Another twist on Harding e-mail breach (John C. Rivard)
- Maybe appalling grammar is bad language design (Don Norman)
- · Wrong credit card in the mail (Stephanie Leif Aha)
- Troubled water crossing bridge (Harald Hanche-Olsen)
- Calling-Number-ID catches obscene caller (Richard R Urena)
- X windows makes patient breathless (Govinda Rajan and Mathew Lodge)
- Trouble in comicland? (Arthur Goldstein)
- Getting help on the Internet (Phil Agre)
- Re: Clipper (Keith Henson, Carl Ellison, Stanton McCandlish)
- COMPUTER RISK! [Early April Fooling?] (Simon Travaglia)

Issue 65 (11 March 1994)

- Using Caller ID to catch obscene callers (anonymous)
- Hard-drive headache (Robert Telka)
- Digital Detritus (Eric Sosman, Stephen D Crocker)
- Re: Maybe appalling grammar is bad language design (Mark Jackson, Alayne McGregor)
- RISK to freedom of information (Philip Overy)
- Re: Clipper (Mark Eckenwiler, Daniel B. Dobkin)
- 13th Intrusion-Detection Workshop (Teresa Lunt)
- First announcement of COMPASS '94, program and info (Teresa Lunt)

Issue 66 (17 March 1994)

- Hit the Wrong Key, become a Verb... (Peter Wayner)
- Aldrich Ames, Master Hacker? (Peter Wayner)
- "Clipper Compromised?" brief in Network World (Christopher Wysopal)
- Sly Imposter Robs S.F. Man of Good Name (Mike Crawford)
- Fire knocks out phone service in LA (George Feil)
- Ease of Administering Phone Systems Leads to Risk of Sabotage (George Pajari)
- Nessy same new trick (Bob Frankston)
- Super-ID and Surveillance (Mich Kabay)
- Caught with their pants down [de-picted by rabbit admirers] (Mich Kabay)

- Neo-nazi T.A.D. eavesdropping (Mich Kabay)
- Derivatives (Phil Agre)
- Followup report on TCAS incident in Portland (Lauren Wiener)
- Caller ID utility (Robert Morrell Jr.)
- New Security Paradigms Workshop: CFP and Correction (Catherine A. Meadows)

Issue 67 (18 March 1994)

- Hazards on the Superhighway (Erskine Widemon)
- The RISKS of whale removal (Tom Mahoney via Mark Stalzer)
- The Handmaid's Tale, Giuliani-Style (Chris Kreussling)
- IRS Surveillance (J. Cooper)
- Risk Conference Two for the price of one! (Patrick J. O'Toole)
- 911 (again) (Richard Johnson)
- Re: Clipper Compromised (Dorothy Denning)
- It's Apple and it's grammar. (John Oram)
- L.A. phone fire (a.k.a. "Risks of believing ...) (Lauren Weinstein)
- RSAREF/RIPEM Free and Legal Worldwide (Jim Bidzos)
- CERT ADVISORY MD5 Checksums (CERT) [Full text in RISKS-15.67MD5]

Issue 68 (22 March 1994)

- Gambling (Phil Agre)
- I really like this guy's attitude (Alan Wexelblat)
- Phone Machines Call Each Other, Part Deux (Russell S. Aminzade)
- IRS Surveillance (Part II) (Zajac)
- Dutch legislators trying to pull a fast one? (Ralph Moonen)
- Funny Money article in THE SCIENCES (Mich Kabay)
- Human Genome Project & Privacy (Mich Kabay)
- SGML--archiving style + content (Mich Kabay)
- Risk of bringing plastic cards through UK customs (Ross Anderson)
- RISKs of safe ATMs (Sidney Markowitz)
- Re: Hard-drive headache! (David M. Miller)
- Re: The RISKS of whale removal, copyrights (Matthew B. Landry, Mark Stalzer)
- Comment on my earlier posting on punctuation and spelling errors (Don Norman)
- Re: Caught with their pants down (Sean Malloy)

Issue 69 (25 March 1994)

- Another ATM failure (with a happier ending) (Mark Connolly)
- Bugs hold up farm cheques (Mich Kabay)
- Nut behind the wheel (Mich Kabay)
- Digital Telephone Switches and Modems (Bob Oesterlin)
- Grammatik bug mistaken for racial putdown (Marni Elci via Roy Beimuts)
- Re: Denver Baggage Handling (John Gersh, Marcus J Ranum, Bear Giles)
- Re: Funny Money article (Sean Eric Fagan, Curtis Jackson, Tobias Ulmer)
- Re: RISKs of safe ATMs (M. Hedlund)
- Re: Comment on earlier [Don Norman] posting (Marcus J Ranum)
- CFP: 2nd ACM Conference on Computer and Communications Security (Li Gong)

Issue 70 (28 March 1994)

- April Fools on the Senate (John Dvorak and Chris Casey via Arthur R. McGee)
- Risks to government (Robert Davis)
- IRS persistence (Dave Methvin)
- BT Billing computers innocent (Marcus Marr)

- Insurance claims ignore patients name (David Bazell)
- The RISKs of Canadian Poodles using 911 (John Oram)
- Ottawa, Canada, Radio contest overloads phone system (Henry Troup)
- 911 as wrong number they don't seem to care anymore (Jeff Hibbard)
- Re: Denver Baggage Handling (Jan Vorbrueggen)
- Re: The RISKS of whale removal (David G. Novick)
- Re: Banknotes and photocopiers (Tom Standage, Padgett Peterson)

Issue 71 (29 March 1994)

- Risks of washroom automation (Paul Colley)
- Pay-per-View failure lets adult station go unscrambled (Mike Carleton)
- Role-playing Addiction (Mich Kabay)
- Software theft statistics (Mich Kabay)
- Risks of spelling checkers (John Girard, PGN)
- Busy-waiting woes (Darren Senn)
- Recent useful newspaper pieces on crypto policy (Lance J. Hoffman)
- Re: L.A. Phone Fire (Nevin Liber)
- Re: Canadian Poodles using 911 (Shawn Mamros)
- Re: Banknotes and photocopiers (Mike Sullivan)
- Re: IRS persistence (Robin Kenny)
- Preliminary Program 7th IEEE Computer Security Foundations Workshop (Li Gong)

Issue 72 (31 March 1994)

- Mud Slide Cuts East Coast Phones (PGN)
- Briton Survives "Monster" Attack due to computer glitch (Will Deatrick)
- Risk Evasion Measures Create New Risks (Stephen A. Stough)
- Rental cars and financial derivatives (Phil Agre)
- White collar crime in Australia (Mich Kabay)
- Hotline reassignment (Mich Kabay)
- Electronic purse (Mich Kabay)
- Dials! (Bob Frankston)
- Re: Spelling Checkers (Geoff Cole, Mary Shafer, Scott A. Siege, Simson L. Garfinkel)
- Disclaimers in software (PGN)
- Junior Exec's Reverse Alchemy (Martin Howard)
- Yet another SSN misuse (Brian Clapper)
- EFF Summary of Public Interest NII Summit 29 Mar 1994 (Stanton McCandlish)

Issue 73 (1 April 1994)

- A320 software goes on "3rd Party" maintenance (Pete Mellor)
- Re: Risks of spelling checkers (Joseph T Chew, Andrea Chen, Eric Sosman)
- Re: Mud Slide Cuts East Coast Phones (David Lesher)
- Aural Sex and Rudder Actuators (A. Padgett Peterson)
- More jail-door openings (Tom Markson, PGN)
- find/xargs strangeness (Peter J. Scott, Chris Dodd)
- P. R. China Computer Security Rules (John Ho)

Issue 74 (2 April 1994)

- Re: Spell checking (J. Taggart Gorman, Pete Mellor, Castor Fu, Les Earnest)
- Re: Language ability is not entirely learned (Paul Colley)
- Re: Spelling, punctuation, poor language technology (Bill Stewart)
- Re: English spelling design (Christopher Upward)

Issue 75 (13 April 1994)

- E-Mail saves a man's life
- Risks of powerful computers to the quality of science (Dan Ruderman)
- Robot mower (Pete Mellor)
- God Grants Granite Gift to RISKS Punsters (Peter Wayner)
- The Soft Pork Underbelly of Efficient Markets (Peter Wayner)
- A creative, HONEST software disclaimer (Neil MacKay)
- E-mail problems (Andrew W Kowalczyk)
- Holiday Inn extra key requirements (Lance A. Brown)
- Fingerprinting & welfare (Mich Kabay)
- Re: More jail-door openings (Al Stangenberger)
- WAIS (Peter Wayner)

Issue 76 (18 April 1994)

- "Friendly Fire" --- U.S. F-15s take out U.S. Black Hawks (PGN)
- The Green-Card Flap
- Data-storage technique provides copy protection (Meine van der Meulen)
- Yet another example of software modification risks (Jim Dukelow)
- Re: Risks ... to the quality of science [randomness] (Steen Hansen)
- MIT student arrested for BBS used for pirate software (Fredrick B. Cohen)
- Credit-Card Fraud (Greg Philmon)
- NII and the US Card (Bill Murray)
- Reckless Baby Bell Marketing (Alan Miller)
- Re: P.R. China Computer Security Rules (Tom Albertson, Dan Sorenson)
- Delayed Dial Tone causes unintentional 911 calls (Chonoles Michael Jesse)
- Seeking lit ref: we trust calculators over ourselves (Mike Crawford)
- Information resource (Michael Enlow)

Issue 77 (19 April 1994)

- Risks ... to the quality of science: Clifford Truesdell (Michael Tobis)
- Dial-in Electric Meter Readings Sans Safeguards (Scott Rose)
- Stun belts -- who has the remote? (Jak Kirman)
- Risks of Data Compression (Joe Decker)
- TV Guide Contest (Agris Taurins)
- Re: MIT student arrest (Dwight Silverman, Sidney Markowitz)
- Re: Green-Card Flap [Risks, Lawyers] (Ed Clarke)
- "Naissance d'un virus" by Ludwig/Condat (Rob Slade)
- IFIP SEC '94 Program (Willis H. Ware)

Issue 78 (22 April 1994)

- Computerized Traffic-Light Problems (Debora Weber-Wulff)
- Risks of winning (Stanley Chow)
- Computer Generates False Tsunami Warning in Japan (George Pajari)
- NYC subway fare cards double-deduct; UI at fault (Andrew Marc Greene)
- A consumer risk from Thomson Consumer Electronics
- Re: we trust calculators over ourselves (John Powell)
- Re: Risks ... to the quality of science (A. Padgett Peterson)
- Re: Risks of Data Compression (John Kennedy)
- Re: Math and money laundering (Erann Gat, Peter Wayner)
- Re: Information resource (Edward Reid)
- Re: Green Card Posting (Caveh Jalali, Ned Kittlitz, Mark Brader)

Issue 79 (26 April 1994)

- Fax programming -- risk to politicians (Tom Keenan)
- Data Escape from Prison (Mich Kabay)
- Industrial espionage (Mich Kabay)
- Trojan @ U. Michigan (Mich Kabay)
- \$14 million QA failure (Mich Kabay)
- Security and Privacy panels (John Rushby)
- Strange Stalking (Flint Waters)
- UK Industrial Spy Law (Peter Sommer)
- Combination Locks I Have Known (Neil McKellar)
- Unusual Newspaper Error (Stewart Rowe)
- Risks of advertising on the net (Jerry Leichter)
- Updated addresses for Canter & Siegel (Paul Robinson)
- Re: MIT student arrested for BBS used ... (Tim Shepard, Douglas Rand)
- Re: NYC subway fare cards double-deduct (Mark Brader, Dan Lanciani, Padgett Peterson)
- Issue 80 (28 April 1994)
 - DMV Computer upgrade goes awry... (Marshall Clow)
 - Time-series wins jackpot (Mich Kabay)
 - Drunk in charge.... (Kearton Rees)
 - Stress Analysis of a Software Project [long] (Tom Davis via Jerry Leichter)
- Issue 81 (29 April 1994)
 - Boot Prom commits Denial of Service Attack (Dave Wortman)
 - Cyrix 486 CPU Bug (Dave Methvin)
 - Call Identifier (tm) forgets list of received calls (Robert Chesler)
 - Re: Unwanted FAX received via voicemail (Declan A. Rieb)
 - Re: Stress Analysis of a Software Project (Tom Davis via Joan Eslinger, A. Padgett Peterson)
 - Inspecting Critical Software (David Parnas via Jan Arsenault)



Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DYGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)

<u>Under Development!!</u>

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

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

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



Search RISKS using swish-e

THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 1

Thurs 2 September 1993

Contents

Is there a roboticist in the house?

Ken Birman

Computer Problems Slow Airline Flights Southern U-S David Fowler

AFSS Computer Crash Knocks Out Service for 12 Hours (July 93)

Dave Barrett

Risks du jour: malpractice; chemical industry vulnerabilities

Phil Agre

Newspaper tide tables

Marc Auslander

Software design [C.A.R. Hoare]

Paul Smee

Re: Cisco backdoor?

Paul Traina

Al Whaley

Easy Access to Video Rental Records

David Jones

Answers to phone-related questions

Lauren Weinstein

Risks of Discussing RISKS

Dennis D. Steinauer

Re: Mars Observer tank testing

Kevin Maguire

Conference on Technology Conversion

Gary Chapman

Info on RISKS (comp.risks)

✓ Is there a roboticist in the house?

Ken Birman <ken@cs.cornell.edu> Tue, 31 Aug 1993 00:39:30 GMT

[Article 2650 (3 more) in cucs.general, sent to RISKS by Li Gong <gong@csl.sri.com>.]

(From the NY Times, Sat. August 28, page 7)
ROBOT SENT TO DISARM BOMB GOES WILD IN SAN FRANCISCO

San Francisco, Aug 27 (AP) -- A hazardous-duty robot malfunctioned Wednesday night and spun out of control in an attempt to defuse an explosive situation. "It was just spinning around, just going wild," said Edward Ellestad, a member of the Police Department's bomb squad. "People were yelling, 'Shut it off!' So we pulled the plug." The police robot, nicknamed "Snoopy", went out of control as officers tried to get it to grasp a pipe bomb found at the C&B Cafe during a raid. "It could have been a lot worse if had picked up the device when it was doing 360's and banging off the walls," Officer Ellestad said.

Kenneth P. Birman, Dept of Computer Science, Cornell Univ., 607-255-9199 Isis Distributed Systems Inc. 607-272-6327, ken@isis.com

Computer Problems Slow Airline Flights Southern U-S

David Fowler <fowler@oes.ca.gov> Wed, 1 Sep 93 18:00:50 PDT

(Hilliard, Florida) -- The Federal Aviation Administration is still at a loss to explain a computer glitch that knocked out a regional air traffic control center in Hilliard, Florida. An FAA spokeswoman says the trouble yesterday caused delays of up to 90 minutes for flights in a large area of the south. No planes or passengers were in danger. In one case, access to a cellular phone may have been key. The head of the local National Air Traffic Controllers Association says one controller used a car phone to contact the Air Force. He wanted to stop a live-fire exercise, because there was no way to control other planes entering the area. The FAA says it does not know what caused the computer problems.

AFSS Computer Crash Knocks Out Service for 12 Hours

Dave Barrett <barrett@asgard.cs.Colorado.EDU> Wed, 1 Sep 93 17:24:21 -0600

[From *AOPA Pilot*, September 1993, page 33]

For a 12-hour period between July 7 and 8, the computers shut down at the Salt Lake City and Atlanta aviation weather processors. As a result, weather information could not be transmitted to the entire automated FSS [Flight Service Station] (AFSS) network, and nearly all AFSSs lost their ability to file flight plons. The system later returned to normal. Apparently, the computer crash was caused by a time-activated virus in the weather processing software. Both processors shut down at the same time.

A separate system--known as Labs--that uses the old, teletype method of transmitting weather data was not affected by the outage. This system, based in Kansas City, continued to provide weather and flight-plan capability to DUAT contractors, private weather vendors, FSSs and those AFSSs with teletype equipment. Labs is not connected in any way to the Salt Lake City and Atlanta

aviation processors.

AOPA [Aircraft Owners and Pilots Association] has recommended that Labs equipment be retained, even though it's a dated system. In addition to its merits as a provider to DUAT and private vendors, the computer crash proved that Labs can be a valuable backup mechanism to the main weather processors.

Risks du jour: malpractice; chemical industry vulnerabilities

Phil Agre <pagre>
Fri, 27 Aug 1993 15:58:41 -0700

The New York Times, August 27, 1993, p. B9, reports on a service in Philadelphia that lets doctors find out whether a patient has filed any malpractice suits. The article discusses the obvious risks and makes it sounds like most doctors are unlikely to be interested. The service also calls to mind the reportedly widespread practice of blacklisting job-seekers who have filed workers' compensation claims.

The *Wall Street Journal*, August 27, 1993, pp. A1, A8, reports on the computer industry's possible vulnerability to disruptions due to the concentration of chemicals firms. In some cases, chemicals used in chip-making and packaging are only produced by a couple of plants, at least one of which is on an earthquake fault in Japan. This is perhaps an instance of "hyperefficiency", the claimed tendency of market economies to expose themselves to excessive disruption from rare but serious events in cases in which companies find it difficult to invest in long-term disaster preparation because of short-term competitive pressures. In this case, many companies are able to reduce overhead and thus cut costs by drastically reducing the number of suppliers they deal with, and growing economies of scale in some kinds of hardware manufacturing may lead to worrisome concentration as well.

The same WSJ (page B1) reports that Steven Spielberg's production company chose the Thinking Machines CM-5 for "Jurassic Park" (in which, of course, it ran some poorly designed software) because it "looked the least like a science-fiction machine". Wow.

Phil Agre, UCSD

Newspaper tide tables

Marc Auslander <marc@watson.ibm.com> Tue, 31 Aug 1993 14:18:55 -0400

The Canberra Times

CORRECTION

For some considerable time, *The Canberra Times* has been publishing the wrong tide times for Narooma. The error has been in arithmetical calculation in this office of the difference between tide times at Fort Denison as published in standard tide tables and times at Narooma. The error, the source of which is lost in antiquity, was discovered last week when the editor, relying on The

Canberra Times figures, was swept out to sea. But he managed to return to shore - and ordered this correction.

Marc Auslander <marc@watson.ibm.com> 914 784-6699 (Tieline 863 Fax x6306)

✓ Software design [C.A.R. Hoare]

Paul Smee <P.Smee@bristol.ac.uk> Wed, 1 Sep 1993 10:16:41 +0000 (GMT)

While clearing out my file cabinet, I uncovered the following, which struck me as relevant to a lot of what goes on in comp.risks. Quoted from a paper, 'The Emperor's Old Clothes', by Charles Antony Richard Hoare, published in CACM Feb 1981:

...there are two ways of constructing a software design: One way is to make it so simple that there are _obviously_ no deficiencies and the other way is to make it so complicated that there are no _obvious_ deficiencies.

The first method is far more difficult. It demands the same skill, devotion, insight, and even inspiration as the discovery of the simple physical laws which underlie the complex phenomena of nature. It also requires a willingness to accept objectives which are limited by physical, logical, and technological constraints, and to accept a compromise when conflicting objectives cannot be met. No committee will ever do this until it is too late.

(The paper was the 1980 ACM Turing Award Lecture. The _'s represent his italics.)

Paul Smee, Computing Service, University of Bristol, Bristol BS8 1UD, UK P.Smee@bristol.ac.uk - Tel +44 272 303132 - FAX +44 272 291576

★ Re: Cisco backdoor? (RISKS-14.87,88,89)

Paul Traina <pst@cisco.com> Fri, 27 Aug 1993 11:37:44 -0700

I just spoke to Al, and found out what the story was. We hired a subcontractor and part of his deal with us is that we provide them access to the Internet through cisco's corporate network. Since we have a relationship and our networks are physically tied together, the routers are specifically configured to allow greater access between our site and theirs (at their request).

There was absolutely positively no "back door." All never actually performed any tests with routers where he knew the configuration, and I would toss the entire thing up to some miscommunication.

★ Re: Cisco backdoor? (RISKS-14.87,88,89)

Al Whaley <Al.Whaley@sunnyside.com> Tue, 31 Aug 1993 23:36:08 -0700 (PDT)

After consulting with Cisco, they have convinced me that the phenomenon I reported earlier in RISKS-14.87 was not a back door but was instead a unique situation to a particular company's equipment caused by an unrelated management issue. The explanation seems reasonable, and I am willing to assume that the supposed back door does not exist at this point, especially since several independent groups have not been able to confirm its existence. Those with Cisco routers can presumably relax, at least as far as this issue is concerned.

Al Whaley al@sunnyside.com +1-415 322-5411(Tel), -6481 (Fax) Sunnyside Computing, Inc., PO Box 60, Palo Alto, CA 94302

[At Al's request, and as a courtesy to CISCO, I have appended a note in the CRVAX ARCHIVE copy of RISKS-14.87 and RISKS-14.89 pointing to THIS issue. Other archive maintainers may wish to recopy those issues. Thanks. PGN]

Easy Access to Video Rental Records

David Jones <djones@cim.mcgill.ca> 2 Sep 1993 12:06:46 -0400

I was in a local "Video Esprit" 24-hour video rental store here in Montreal and I noticed a new service they have added for their customers. There is a PC in the store that, among other things, allows you to review your own "rental history". To access your records you just type in the last several digits from your membership card.

Since the issue of privacy of video rental histories has had much discussion, I thought RISK readers might be interested to know just how *easy* it has become to get a list someone else's video rentals. Just a glance at their membership card is all it takes.

David Jones

answers to phone-related questions

Lauren Weinstein <lauren@vortex.com> Fri, 27 Aug 93 12:43 PDT

A couple of telephone-related questions popped up in the digest, and while they might more properly be answered over on TELECOM, here are a couple of answers anyway:

1) Dial 1 first. This is becoming universal in North America to

provide a sure way to distinguish between areas codes and prefixes. The network can only provide you with a recording that tells you that you need to dial 1 so long as no duplicate codes exist that will interfere with parsing of a particular call. Many metro areas for years have been assigning prefixes that duplicate area codes. Without 1+ dialing, the only way to differentiate would be by counting digits and providing long timeouts at the end of dialing all calls to determine when no more digits will be forthcoming.

Starting around 1995, when the conventional area codes (second digit 0 or 1) run out, new area codes will be assigned that look like prefixes. The potential problems that may result in some phone systems, PBXs, etc. are quite nasty due to programmed (and in some cases hardwired) limitations in number parsing.

The days when dialing 1 meant "toll call" are long since past in most areas, and will be gone everywhere quite soon.

2) It has long been understood that using the same code (e.g. *67) for both blocking *and* unblocking of calling number ID is a bad idea. Bellcore originally assigned the single code, and various telcos have argued before state commissions that there are various technical reasons why they couldn't have separate codes with existing switch software (generics). However, my understanding is that most of the major switch generics are in the process of being updated to allow this, and then those "technical" arguments will presumably no longer hold much sway in the discussion.

The issue of calling number delivery via ANI (e.g. 800 numbers) is a complex one. It can be argued that calling an 800 number is like making a collect call--the party you're calling is paying for the call, and they need to know who is using their resources (either correctly or abusively) and where their money is going.

Both of these issues are probably better followed-up over in TELECOM or other telecommunications-specific forums.

--Lauren--

Risks of Discussing RISKS

Dennis D. Steinauer <dds@csmes.ncsl.nist.gov> Mon, 30 Aug 93 15:57:46 EDT

Is discussing risks RISKY? I would like to see more discussion of this topic -- even though it's been discussed in years past. I agree completely with PGN, who suggests that many people (I'd argue the majority) are living with blinders on. Even those on the provider/vendor side who should understand the risks of certain technologies (cellular phones being an obvious example), have a) underrated the intelligence of potential adversaries, b) overestimated the cleverness of their own technology, c) underestimated the speed at which exploitation information and devices would be

disseminated, d) assumed that the using public can't be hurt by what they don't know, and e) let the magnitude of the financial rewards overshadow everything. Perhaps, more open discussion -- and knowledge that such discussion -was- going to happen -- would encourage providers not to make naive assumptions regarding the risks and might cause users to demand more of the products they buy. (Where have we heard that before?)

Anyway -- one approach to the problem has developed over the last few years (since the Internet worm incident, to be more precise) that might be worth noting. A voluntary cooperative group of security incident response teams known as FIRST (Forum of Incident Response and Security Teams) has developed to address the problem of sharing potentially risky information without giving away the store in the process. Member teams include response teams representing a wide range of "constituencies", including the Internet (i.e., CERT), various government agencies (e.g., DISA/ASSIST for DoD, Dept of Energy's CIAC, CCTA for the UK, SurfNET in the Netherlands, etc.), private sector organizations, vendors, and academia. Member teams share information on both latent and active system vulnerabilities through a series of alerts issued by the various teams. The alerts attempt to walk the fine line of describing a problem in sufficient detail (along with corrective actions) without providing enough information for exploitation. By initially distributing alerts only among member teams (and careful vetting of members), there is reasonable control over distribution.

This certainly has not solved the problems associated with identifying and closing system or network risks, it has made, I believe, great strides toward building trust and mutual support through effective information sharing and cooperation. Other groups have use a similar approach to address similar problems -- e.g., the sharing of virus information. I would be quite interested to hear how others have addressed the problem.

★ Re: Mars Observer tank testing (Stern, RISKS-14.89)

Kevin Maguire <maguire@zappa.Jpl.Nasa.Gov> Mon, 30 Aug 93 14:32:30 PDT

- > Apparently the tank pressurization system on the Observer was tested
- > exactly once, and it "blew up." Whether this phrase is meant to imply
- > an explosion or merely a bad leak is an exercise left to the reader.

This is hardly a suspicious occurrence. Testing of a new pressure vessel design always includes, as a matter of standard practice, testing to failure. This testing is required to ensure that the burst pressure is where analysis indicated and that it is far enough removed from the operating pressure.

What would have been suspicious is if this test had NOT been performed.

Kevin Maguire maguire@zappa.jpl.nasa.gov

[It is my understand that standard procedure is to limit-test the FIRST tank to see how far it can be stressed, that is, stressed to the point

at which it actually blows. That is clearly not a test one wishes to do on many tanks. It also tells you nothing about other tanks. PGN]

Conference on Technology Conversion [long]

Gary Chapman <chapman@next1.harvard.edu> Wed, 01 Sep 1993 14:57:36 -0400 (EDT)

****PLEASE CIRCULATE THIS MESSAGE TO INTERESTED PARTIES****

The 21st Century Project and the National Commission on Economic Conversion and Disarmament are co-sponsoring the National Conference on Technology Conversion: Reinvestment in National Needs. What follows is a schedule of speakers for the conference, which will be held October 7th and 8th in Arlington, Virginia. Anyone interested in the subjects that will be covered at this conference is encouraged to register and attend.

Gary Chapman, Coordinator, The 21st Century Project, Cambridge, MA chapman@next1.harvard.edu

National Conference on Technology Conversion: Reinvestment in National Needs

October 7-8 Roslyn Westpark Hotel Arlington, VA

Speakers will include representatives from:

The 21st Century Project
American Capital Strategies
Cray Research Corporation
Computer Professionals for Social Responsibility
Department of Energy
Economic Policy Institute
Federal Highway Administration
Federation for Industrial Retention and Renewal
Industrial Union Department, AFL-CIO
International Association of Machinists
Microelectronics and Computer Corporation
National Economic Council
National Institute of Standards and Technology

Northrop Corporation
Congressional Office of Technology Assessment

Sun Microsystems

Toxics Use Reduction Institute

United Technologies Corporation

White House Office of Science and Technology Policy

Westinghouse Electric

World Resources Institute

Worldwatch Institute

The National Commission for Economic Conversion and Disarmament will convene a conference on a major aspect of the conversion challenge:

- 1. To redirect our military-oriented federal science and technology policy toward solving our neglected domestic problems
- 2. To promote investments in emerging technologies that can create new jobs and market opportunities for converting businesses
- 3. To explore the means of financing technology conversion
- 4. To democratize the policymaking process.

The conference will bring together policy makers within the Administration and Congress, scientists and engineers, corporate managers and trade unionists, and those in the independent sector working on issues of conversion, the environment, renewable energy and transportation policy.

In plenary sessions we will examine current science and technology policy, the missing pieces of this policy, and the means of financing investments that will turn emerging technologies into sustainable, life-affirming enterprise. In working groups we will look more closely at some of the most promising of these technologies.

Conference Co-Sponsors include:

Economic Policy Institute
Industrial Union Department, AFL-CIO
Energy Conversion Devices, Inc.
University of Wisconsin Extension/ School for Workers
The 21st Century Project

II. Registration Information

To register by mail send a check for \$80, payable to ECD, to: ECD, Suite 9, 1801 18th Street, NW, Washington, D.C. 20009. Your registration fee covers lunch and break refreshments on both days and refreshments at the October 7 reception (there will be a cash bar).

A small number of rooms have been reserved for conference participants at the Westpark Hotel, at a reduced rate of \$87.00 per night. For reservations call (703) 527-4814 or (800) 368-3408. The Westpark Hotel is located at 1900 North Fort Myer Drive, Arlington, VA, one block from the Key Bridge and the Roslyn Metro Stop; on the Blue Line from National Airport.

Space is limited, so please make reservations early. If you have any s regarding the conference, please call Miriam Pemberton, Jim Raffel or Kristen Kann at 202-462-0091.

On the afternoon of October 8th we will hold 12 workshops on emerging technologies, four at a time. To help us schedule these to accommodate conference participants best, please indicate the three workshops that you are most interested in attending when registering:

- A. Fuel Cell Technology
- B. Renewable and Alternative Energy Technology
- C. Transportation Technology
- D. Environmental Technology
- E. Aerospace Technology Markets
- F. Infrastructure Development
- G. Smart Materials Technology Implementation in Infrastructure Enhancement
- H. High Speed Rail and Freight Transportation
- I. Zero-Discharge Manufacturing Technology
- J. Information Infrastructure
- K. Shipbuilding Industry
- L. Manufacturing Extension Services
- III. Preliminary Conference Schedule

THURSDAY, OCTOBER 7, MORNING SESSION

Plenary I - Conversion and National Science & Technology Policy

1. Introductory Remarks:

Senator Barbara Boxer, (D-CA) (invited)

Katherine Gillman, Special Assistant for Defense Conversion, White House Office of Science and Technology Policy

Ann Markusen, Professor, Rutgers University; co-author of Dismantling the Cold War Economy

2. Redefining National Security: Federal Policy in the Post-Cold War Era

George Brown (D-CA), Chair, House Science, Space and Technology Committee (invited)

Vice President Albert Gore, Jr. (invited)

Seymour Melman, Chair, National Commission for Economic Conversion and Disarmament

3. Dual-Use Technology Policy and Beyond

Dorothy Robyn, National Economic Council

Lewis M. Branscomb, Albert Pratt Public Service Professor, John F. Kennedy School of Government, Harvard University

4. Technology Transfer

Rep. Ron Wyden, (D-OR)

Robert D. Glasser, Center for National Security Studies, Los Alamos National Laboratory

Jim Ling, Science, Technology and Public Policy Program, MIT

THURSDAY, OCTOBER 7, AFTERNOON SESSION

Plenary II - Reinvestment and Conversion: Toward a National Needs Agenda

1. Environmental Sustainability

Michael Renner, Senior Researcher, Worldwatch Institute

Greg Pitts, Microelectronic and Computer Technology Corporation

2. Economic Conversion

Peter diCicco, Secretary Treasurer, Industrial Union Department, AFL-CIO

Rep. Rosa DeLauro, (D-CT) (invited)

Lou Kiefer, International Association of and Aerospace Workers

Joseph Hoffman, Manager of Marketing Systems Development and Engineering Division, Westinghouse Electronics Systems Group

3. Democratizing the Decision-Making Process

Gary Chapman, Director, 21st Century Project, a nationwide effort to reorient public support for science and technology toward solving critical domestic problems

Jim Benn, Federation for Industrial Renewal and Retention (FIRR)

4. Reception (Thursday Evening)

FRIDAY OCTOBER 8, MORNING SESSION

Plenary III: Technology Innovation and Infrastructure Development

1. Government Initiatives and Institutions

Jeff Faux, President, Economic Policy Institute

Herb Whitehouse, Whitehouse Fiduciary Advisers

2. Private Financing

Bruce R. Guile, Director, Programs, National Academy of Engineering, Washington, DC; tax credits and incentives for innovation and new technology R&D

Tom Schlesinger, Southern Finance Project

3. Alternative Financing Structures

Martin Trimble, National Association of Community Development Loan Funds

Mike Locand Associates, economic consulting firm specializing in conducting feasibility studies for employee buyouts, with a concentration on the steel industry

Adam Blumenthal, Vice President and Partner, American Capital Strategies

FRIDAY, OCTOBER 8, AFTERNOON SESSION

Workshops on the Following Emerging Technologies:

A. Fuel Cell Technology

William J. Lueckel, Vice President, Government Programs and Marketing, International Fuel Cells, United Technologies Corporation

Jeff Serfass, Exec. Dir., Fuelion Group

B. Renewable and Alternative Energy Technology

Eric Vaughn, President, Renewable Fuel Association

Frank Bruno, CEO, Turbo Power and Marine Systems, Inc., division of Pratt Whitney (invited)

C. Transportation Technology: Vehicles, Highways and Public Transit

Victor S. Rezendes, Director, Energy Issues, GAO; on flexible fuel vehicle program

Wesley B. Truitt, Deputy Manager for Business Development, Northrop Corporation

D. Environmental Technology

David Blaskovich, Senior Director, Programs, Cray Research Corporation

Mark Schaefer, White House Office of Science and Technology Policy

R. Darryl Banks, Program Director, Program in Technology and Environment, World Resources Institute

Clyde Frank, Deputy Assistant Secretary for Technology Development, Office of Environmental Management, Department of Energy

E. Aerospace Technologies

David P. Radzanowski, Analyst in Aerospace Policy, Science Policy Research Division, Congressional Research Service

Samuel N. Goward, Associate Professor, Director, Laboratory for Global Remote Sensing Studies, University of Maryland at College Park

F. Infrastructure Development

Harry B. Caldwell, Office of Policy Development, Highway Needs and Investment Branch, Federal Highway Administration

Sue McNeil, Carnegie-Mellon University; infrastructure management, condition assessment, and image processing

G. Smart Materials Technology Implementation in Infrastructure Enhancement

Craig A. Rogers, Professor and Director, Center for Intelligent Material Systems and Manufacturing, Virginia Tech

Vijay Varadan, Professor of Engineering Science, Pennsylvania State University and Editor-in-Chief, Journal of Smart Materials and Structures

H. High Speed Rail and Freight Transportation

Raymond V. Lanman, National Railroad Passenger Corporation (Amtrak); commuter rail and business development

Edward K. Morlok, University of Pennsylvania; freight transportation in the future: New Demands, New Approaches, New Technologies

John Ullmann, Professor of Management and Quantitative Methods, Hofstra University

I. Zero-Discharge Manufacturing Technology

Robert Atkinson, U.S. Congress, OTA, Industrial Technology & Employment Program

Ken Geiser, Director, Toxics Use Reduction Institute at U Mass, Lowell

J. Information Infrastructure

Marc Rotenberg, Washington Office Director, Computer Professionals for Social Responsibility

John Gage, Sun Microsystems (invited)

K. Shipbuilding Industry

William Avery, Johns Hopkins Applied Physics Laboratory; expert on Ocean Thermal Energy Conversion

Virgil Rinehart, Senior Advisor for Shipbuilding, Maritime Agency

L. Manufacturing Extension Services

Philip Nanzetta, Director, Manufacturing Extension Partnership, National Institute of Standards and Technology

George Sutherland, Director, Great Lakes Manufacturing Technology Center



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 2

Friday 3 September 1993

Contents

BETTER airline/travel-agent computer hide-and-seek

Mark Seecof

Lost Canadian crime statistics data

Luis Fernandes

Risk of incorrect Daylight Saving conversion

Arthur David Olson

The Risk of Discussing "the risks of discussing risks" in RISKS

Jeffrey S. Sorensen

The risks of CERT teams vs we all know

Fredrick B. Cohen

Potential risk in terminal buffer storage

Robert S. Richardson

Electronic documents

Mich Kabay

Re: Dorothy Denning and the cost of attack against SKIPJACK

Bill Murray

Re: Mars Observer tank testing

Donald Arseneau

Re: Dial 1 first

Mark Brader

COMPASS '94 CALL FOR PAPERS

John McLean

Info on RISKS (comp.risks)

✗ BETTER airline/travel-agent computer hide-and-seek

Mark Seecof <marks@wimsey.latimes.com> Thu, 2 Sep 93 20:22:54 -0700

On page B-1 of the Wall Street Journal, 1 Sep 93 a story headlined "Fliers find scarcity of choice seats" by James Hirsch describes how major airlines are now manipulating seat assignments in coach class to favor frequent flyers and full- fare passengers. They manage this through their computer reservation systems (CRS's). Some travel agents are struggling to get good

seats for their disfavored clients by fooling the CRS's or even by using other computers to poll CRS's looking for "openings" to reassign better seats to their clients.

[What follows is Seecof's appreciation of the story, not quotation; errors and opinions belong to Seecof.]

Airlines used to give out coach seats on a first-come-first-served basis. Other classes of ticket (1st, business) got different, better seating. But not all coach seats are equal in flyers' eyes: people prefer aisle or window seats near the front of the cabin. Airlines in search of ways to differentiate their service are now giving "full-coach" (fare) and very-frequent-flyer passengers the better seats. However, they have not announced their policy to the public. Instead, people holding low-fare tickets who request seat assignments are told that the good seats are already taken--and are offered less desirable seating. Depending on how the message is phrased, it comes across as baffling ("the seats are unavailable") or misleading ("the seats are already assigned"). Travel agents can figure out which seats are really assigned by testing different sample data against the seat assignment algorithm for each flight in a CRS... if an agent tries to seat a passenger on a cheap ticket and is told that only middle seats at the rear are available, he can attempt to reserve seats for a hypothetical full-fare passenger to see which seats will be available to such a flyer. According to Hirsch, many airlines "free up" unfilled-but-restricted better seats as departure time approaches so that late-booking flyers can get seat assignments.

According to the WSJ, some travel agents are retaining the frequent-flyer ID's of favored passengers and using those to reserve seats for less favored flyers. Agents also apply other schemes--including booking a flight on a full-fare ticket, then later revising the reservation to a lower-fare ticket. Associated Travel Management, of Santa Ana, Calif. is said to use a proprietary computer system which monitors the availability of seats for specified flights and passengers by polling a CRS--when a "better" seat "becomes available" the system requests it for the client passenger. A client may have his seat changed many times without human intervention as the system grabs seats grudgingly offered by the CRS. The WSJ says the airlines don't like travel agencies bucking airline seat assignment algorithms.

This is fascinating. Leaving aside the irritating deception practiced by the the airlines (they avoid telling low-fare passengers *why* they can't get good seats), the seat-assignment algorithms are perfectly rational--you want a good seat, you gotta pay more. (You may wonder why the airlines don't break out the price of better seats--just charge 5% more for good seats. I think it's 'cause they don't want to give full-fare passengers discounts for bad seats. When a 'plane is full even favored passengers can be assigned bad seats--if the seat price differential were explicit on the up-side, those flyers would demand reciprocal discounts on the down-side.) The travel agents' tactics are also rational--the CRS gives good seats to reservations with certain qualities... then tell the CRS what it wants to hear! But the travel agencies are forced into either deceiving the CRS on behalf of flyers (by falsely claiming that the flyer will pay full fare, or is a very frequent flyer), or using computers of their own to tussle with the CRS for seats. If agencies other than Assoc. Travel Mgmt. start to use similar systems to try

and get good seats for their clients, seat assignments could become a kind of lottery. With many agent systems polling a CRS looking for a seat, when they all try to pounce on one at the same time it'll be chancy which transaction gets through.

I see two risks arising from the way airlines and travel agents are exploiting computers to complicate seat assignment. The first is, that travel agents and flyers generally are being taught to lie to the CRS's. That is, a premium has been placed on falsifying input data to the computer. Now, people gain economic advantage by lying all the time. But in this case they are lying at low or zero (depending on the exact tactics they adopt) risk and in a situation where their conscience does not bite. Before computers, you had to lie to a human being and unless you were a sociopath you probably felt guilty about it. Now a computer has been programmed to implement a sufficiently harsh seating regime that you feel prompted to lie your way past it (especially since the airlines are lying to you about the price differential for good seats--because they don't want to discount bad ones), and you are not likely to feel any guilt over lying to a computer, a mere machine, albeit there are human consequences downstream--those are very remote. The effect of lying to the machine is GIGO--you provide bad input, the machine provides bad output. Airlines will find that their revenue estimates are wrong, because many full-fare bookings will be mere subterfuges to obtain good seats, and so-on down the line. To avoid this, airlines will design and implement complex, costly, and likely quite punitive algorithms to validate input more effectively. This will prompt even more sophisticated schemes to evade those algorithms, likely by more subtle input data distortion...

The second risk is that only flyers using agents with systems designed to beat on a CRS until it coughs up a desired seat will get good seats. This will harm flyers without such agents, and prompt the development of more such polling systems. As that in turn loads down CRS's they will cost more to run, and unless they are reprogrammed, seat assignment will become like a lottery; which many flyers will think less fair than either first-come-first-served or pay-more get-more. Either way, costs will be passed on to flyers whether or not they use agents with fancy CRS-pounding systems.

In the final analysis it might be cheaper for airlines and flyers both to use a simple seat-assignment scheme with more perceived fairness and skip the whole computer arms race.

Mark Seecof <marks@latimes.com>

Lost Canadian crime statistics data

luis fernandes <elf@ee.ryerson.ca> Fri, 3 Sep 93 17:25:59 EDT

Toronto Star, Aug. 31, 1993 [p. A9]

TORONTO-- Statistics Canada reported a dramatic drop- almost 12 percent- in violent crime across Metro from 1991 to 1992. But according to Metro police, violent crimes [assault, sexual assault, robbery, etc.(!)], except

homicides, continued to climb last year. For example, Statistics Canada cited 24,408 assaults (both sexual and non-sexual) in Metro last year...But the Metro police annual report cited 29,071 assaults reported last year...

Officials at Statistics Canada and Metro police could not explain the discrepancies yesterday. A Statistics Canada official said the figures were provided by Metro police...

The next day (Sept. 1, 1993), the following report appeared [p. A2]:

Statistics Canada has likely lost computer data, causing a major miscalculation of Metro's violent crime rate, Metro police say...

Puzzled StatsCan officials said they may know today what's wrong.

[Gordon MacKay of the Canadian Centre for Justice Statistics, which compiled the figures for StatsCan] said that one possibility is a problem with data they received via a recently installed computer link-up.

Both Metro police and Statistics Canada officials said yesterday there were no problems when the calculations were done manually from typed reports.

This year's federal crime survey marked the first time Metro's figures were calculated using computer tapes provided by the force. The system was supposed to speed-up calculations and do away with paperwork...

MacKay said StatsCan usually sends preliminary findings to each police force for verification. But Metro police didn't receive the crime figures from the agency until yesterday-- hours after it had made its findings public, [said Mike Dear, Metro police's director of records and information security.]

The Thursday edition did not follow-up.

[An earlier problem with the Metro Police handling of crime data was contributed by Doug Moore to RISKS-14.18. PGN]

✓ Risk of incorrect Daylight Saving conversion (Eggert, RISKS-14.87)

Arthur David Olson <ado@elsie.nci.nih.gov> Mon, 30 Aug 93 15:09:43 EDT

Paul Eggert's note that

On August 28, 1993, at 2 AM local time, workstations and PCs in Israel that are running Sun's Solaris 2.2 will suddenly lose an hour.

might be riskier than expected. Several years ago Mubarak Awad was one of the Carey Memorial Lecturers at Baltimore Yearly Meeting of the Religious Society of Friends (Quakers); a transcript of the lecture should be available from the yearly meeting. Mubarak stated that as a form of resistance some Palestinians used their own rules for starting and ending Daylight Saving Time, and that folks whose watches ran on Palestinian time risked having them broken if stopped for questioning.

Arthur David Olson ado@elsie.nci.nih.gov

★ The Risk of Discussing "the risks of discussing risks" in RISKS

Jeffrey S. Sorensen <sorenjs@pb.com> Fri, 3 Sep 93 13:43:21 -0400

The discussion of the risks of discussing risks in RISKS is not without its risks. I am very meta-concerned with this issue. Remember that excessive scrutiny of a digest like RISKS might, in the process of debate, provide material for those who would censor such a discussion. If we, even momentarily, entertain the notion that RISKS is perhaps a hotline for crackers to exchange tips, many administrators may try to limit distribution without waiting for the discussion to end.

There is also the _even greater_ danger of being caught in an infinite regress until every megabyte of space on the net is filled with the text "risks of risks of risks of risks..."

Or even _worse_, some readers may find the discussion of the discussion of risks to be so abstract and pointless that they unsubscribe to this group as they are reading this sentence. We must balance the risk of discussing risks against the risks of alienating RISKS readers.

Jeff Sorensen sorenjs@pb.com

The risks of CERT teams vs we all know

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Fri, 3 Sep 93 06:08:16 PDT

The problem with restricting information to CERT teams, etc. is that this:

- 1 creates a techno-elite
- 2 limits distribution far too much

I expand upon it:

Creating a techno-elite makes it impossible for the average peerson or the interested novice to get involved. Most of the major breakthroughs in information protection ever the ages have come from one of these types and NOT from the techno-elite. We are creating an inbreeding situation that could be a fatal flaw.

Limiting distribution to these groups means that the vast majority of those who actually perform these protection functions are denied the facts they need to get the job done. Suppose the attacker takes out the phone lines to your CERT. You become hopeless because you are a sheep. If you know how things work on your own, at least you have a chance to defend yourself.

 FC

P.S. In my exchange, you may not dial a 1 for local calls, and you must dial a 1 for non-local calls EXCEPT for international call. Dialing a 1 before everything doesn't work. Does anyone have a universal list of exchanges and which other exchanges are considered local to them? I think not! Without this, how can I automate the process? Wait for a disconnect and assume it was from a failure to dial/not dial a 1?

Potential risk in terminal buffer storage

"robert s. richardson" <bob@CSOS.ORST.EDU> Fri, 3 Sep 1993 01:28:07 -0700 (PDT)

I use a terminal program on my computer that automatically allocates free memory as you use it to store a copy of your on-line session. I have this buffer configured rather large (about 1/2 meg) so that I may scroll back through news and such if I remember I point I want to look up. The other day a co-worker used my terminal for a couple of hours, then I took over again. I went to check the buffer for something I was doing, and noticed that a copy of their entire session, which included email and other personal and business related items I should not have had access to, were in the buffer. I deleted the buffer immediately, but the potential RISK here is that if you are using an unfamiliar terminal, or even you own, it is possible that information you or others wish to be secret can be sitting in a buffer for hours or even days. Flush that buffer at the end of each session!

Bob Richardson, OmiCo Industries, PO Box 1404 Corvallis, OR 97339 bob@kira.csos.orst.edu 503-758-5018

✗ Electronic documents

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 03 Sep 93 07:52:52 EDT

A recent article deals with several RISKS of depending on electronic documents:

Hayes, B. (1993). The electronic palimpsest; Digital documents for all occasions: erasable, correctable, reproducible, forgeable. _The Sciences_ (NY Academy of Sciences) 33(5):10.(Sept/Oct 1993)

I enjoyed reading Brian Hayes article in the new issue of this fine magazine. It is not only informative and up to date, but also elegant, amusing and beautifully illustrated with various paintings. Summary follows:

"As a writing instrument, the computer is not su much a better pencil as a better eraser." You can eliminate all traces of your early versions at the stroke of a key.

This easy erasability leads to difficulties of authentication. How can one prove who wrote an electronic document? Digitized signatures make the problem

worse, since anyone can scan a real signature and then print in on any document. However, digital signatures are a good method of authentication. The public key cryptosystem allows you to encrypt a document with your private (secret) key; only the corresponding public key decrypts the message. The encrypted version is as big as the original, though: a nuisance. A refinement, the digital signature, encrypts a digest of only 160 bits and provides the same confidence of authentication.

Another problem is forgery. If we pay the rent with an electronic cheque, what stops a crook from using copy after copy of the same cheque? We will need unique serial numbers on electronic cheques.

What about proving _when_ a document was created? Here we have to rely on a time-stamping service. Scientists at BELLCORE have invented the time-stamp equivalent of the digital signature. You submit a digest of the document that needs to be time-stamped to a trusted time-stamping computer; it generates a cryptographically-sound certificate which includes the time of receipt.

To prevent fraud at the time-stamping computer (where someone might change the system clock long enough to produce fake time-stamps for a specific crime), every certificate is merged mathematically with all the others issued during the same weekly period. The summary time-stamp is then published in _The New York Times_.

The legal system will have to adapt to the increasing use of electronic documents. Historians will also have more trouble piecing together the creative process if only the final version is published or physically available. And what about the rapid changes in computing technology and storage devices? Who will be able to read today's diskettes a hundred years from now? Or even ten? Archivists must think about these issues.

<

★ Re: Dorothy Denning and the cost of attack against SKIPJACK

<WHMurray@DOCKMASTER.NCSC.MIL> Thu, 2 Sep 93 22:20 EDT

On page 14 of the August 30, 1993 issue of Government Computer News, Kevin Power reports that Dorothy Denning told the Computer System Security and Privacy Advisory Board that SKIPJACK would not be compromised by exhaustive attack methods in the next 30 to 40 years.

I am reminded of a story, perhaps apocryphal. In the middle seventies Fortune magazine was working a feature on computer crime. Most of the experts that they interviewed told them that the security on most of the nation's commercial time sharing systems was pretty good. However, they admitted that one convicted felon and hacker, Jerry Schneider, would tell them otherwise. Of course Fortune had to interview him. According to the story, the interview went something like this:

Fortune: Mr. Schneider we understand that you are very critical of the

security on the nation's commercial time sharing systems.

Jerry: Yes, that is right. Their security is very poor.

Fortune: Could you break into one of those systems?

Jerry: Yes, certainly.

Fortune: Well, could you demonstrate for us?

Jerry: Certainly, I'd be happy to.

At this point Jerry took the reporters into the room where his "Silent 700" terminal was. He connected to the system that he normally used but deliberately failed the logon. When he deliberately failed again at the retry prompt, the system disconnected. Jerry dialed in again, failed a third time, and this time he broke the connection. He dialed a third time but this time he dialed the number of the operator.

Jerry: This is Mr. Schnieder. I seem to have forgotten my password. Can you help me?

Operator: Sorry Mr. Schnieder, there is nothing that I can do. You will have to call back during normal business hours and talk to the security people.

Jerry: I am sorry too, but you do not seem to understand. I am working on something very important and it is due out at 8am. I have to get on right now.

Operator: I am sorry. There is nothing that I can do.

Jerry: You still do not understand. Let me see if can clarify it for you. I want you to go look at your billing records. You will see that you bill me about \$800- a month. This thing that I am working on; it is why you get your \$800-. Now, if you do not get off your a-- and get me my password so that I have this work out at 8am, by 9am there is going to be a process server standing on your front steps waiting to hang paper on the first officer through the door. Do I make myself clear?

Apparently he did.

Operator: Mr. Schnieder, I will call you right back.

At this point he appears to have one or two things right. He changed the password, called Jerry back at the number where his records said that he should be, and gave him the new password. Jerry dumped two files and then turned to the reporters. With a triumphant smile he said "You see!"

Fortune (obviously disappointed): No, No, Mr. Schneider! That is not what we wanted to see. What we wanted to see was a sophisticated penetration of the software controls.

Jerry: Why would anybody do THAT?

The cost of an exhaustive attack is an interesting number. It gives us an upper bound for the cost of efficient attacks. However, it is never, itself, an efficient attack. It is almost always orders of magnitude higher than the cost of alternative attacks. The very fact that its cost can be easily calculated ensures that no one will ever encrypt data under it whose value approaches the cost of a brute force attack.

History is very clear. "Black Bag" attacks are to be preferred; they are almost always cheaper than the alternatives. After those are attacks aimed against poor key management. These attacks will be very efficient when the keepers of the keys already work for you and where their continued cooperation and silence are assured.

William Hugh Murray, 49 Locust Avenue, Suite 104; New Canaan, Connecticut 06840 1-0-ATT-0-700-WMURRAY; WHMurray at DOCKMASTER.NCSC.MIL

★ Re: Mars Observer tank testing (RISKS-15.01)

Donald Arseneau <asnd@erich.triumf.ca> Fri, 03 Sep 1993 01:25:19 PST

> It [testing to destruction] also tells you nothing about other tanks. PGN

What a silly statement! It tells you a lot: it says the design is not completely wrong; it says that the manufacturing can be done properly; it even says that another tank, made the same way without error, will work.

Maybe Peter is too absorbed in software validation lately, where his strong statement may be true.

Donald Arseneau asnd@reg.triumf.ca

[I was obviously a little less than precise.

Destruction testing tells you something about the fabrication process and, yes, it tells you something about the design.

Its usefulness assumes that there were no design changes between tanks, and no changes in the fabrication process.

But it does not tell you that the second tank does not have an implementation flaw. Yes, I need to be very precise. So do the tank fabricators. T'anks. PGN]

Re: Dial 1 first (Cohen, RISKS-14.89)

Mark Brader <msb@sq.sq.com> Fri, 27 Aug 1993 23:10:59 -0400

This topic arises in comp.dcom.telecom as regularly as its moderator lets it in there. For the benefit of foreign readers, this pertains to a significant variation in the methods of dialing phone calls in different parts of the US and Canada. In some areas, a leading 1 in a number means that an area code

follows; in others, the ones discussed here, it means that the call is long distance. These two ways of classifying a call are in general independent of each other. Further variations, not discussed here, applies to exactly when you have to dial the area code.

> Until recently, I had the good fortune of living in a telephone > exchange without this problem ...

It's not a bug, it's a feature. (But see below.)

- > Why do I have to dial 1 before some numbers and not before others?
- > The computer at the phone company politely tells me to dial 1 first, or
- > to not dial 1 first depending on where the call is made to, but this is
- > little comfort for my autodialer making a series of several thousand calls
- > to send out FAXes. If they can tell me to add 1 or not, why can't they just
- > add it or not for me?

Because, in places where the rule is "dial 1 first if and only if the call is long distance", it is assumed that

- (1) nobody wants to dial a long-distance call by accident
- (2) everybody knows what numbers they can reach with a local call and (3) local and long distance are the only kinds of calls.

Assumption 1 justifies the "dial 1 if it's long distance". Assumption 2 justifies the "only if" part of the rule, because of this reasoning: if you dialed a local number *with* the 1, then you must obviously have meant to dial some *different* number which would *not* have been local.

I said it was a feature, and for some people it is. For others, such as Mr. Cohen, it is a major nuisance. It's even worse for people who regularly travel about and take modems with them and want to program phone numbers into the modems.

Modern phone systems should be able to configure one or another dialing method according to the *customer's* preference, but nobody has offered such a feature. I suspect the view is that either there would be little demand or that people would find it too confusing when using a phone not their own. (Yet, from my office, I have to dial 9 for a local call, and 81 for long-distance...)

There are also places where the rule is implemented incompletely, either because assumption 3 does not hold or due to some local quirk. These, I suspect, are a nuisance to everybody.

Mark Brader, SoftQuad Inc., Toronto utzoo!sq!msb, msb@sq.com

✓ COMPASS '94 CALL FOR PAPERS

<mclean@itd.nrl.navy.mil>
Mon, 30 Aug 93 16:41:43 EDT

CALL FOR PAPERS COMPASS '94

9th Annual IEEE Conference on COMPuter ASSurance

June 27-30, 1994 Gaithersburg, MD

The purpose of this conference is to bring together researchers, developers, and evaluators who work on problems related to specifying, building, and certifying high-assurance computer systems. What distinguishes COMPASS from similar conferences is its emphasis on bridging the gap between research and practice. Researchers are provided an opportunity to present results, new theories, and new technologies to both other researchers and practitioners who can put them to practice. They can also learn from practitioners of new research problem domains and of problems encountered in building real systems. Practitioners have an opportunity to share lessons learned, to learn of new research, and to influence future research.

Papers should present advances in the theory, design, implementation, evaluation, or application of high-assurance systems, or report on experiments, evaluations, and open problems in the use of new technologies for computer assurance. Special consideration will be given to presentations (either single papers or paper pairs) by practitioners and researchers who have worked on the same problem. There will also be a tools fair. Papers, panel session proposals, tutorial proposals, and tools fair proposals are solicited in the following areas:

Software Reliability
Formal Methods
Real-Time Systems
V&V Practices

Software Safety
Tools
Process Models
Embedded Systems
Standards

INSTRUCTIONS TO AUTHORS:

Send five copies of your paper, panel session proposal, tutorial proposal, or tools fair proposal to John McLean, Program Chair, at the address given below. Abstracts, electronic submissions, late submissions, and papers that cannot be published in the proceedings will not be accepted. Papers submitted from outside North America should be sent via overnight courier service.

Papers must be received by January 15, 1994 and must not exceed 7500 words. Authors are responsible for obtaining prior to acceptance any and all necessary clearances for publication. Authors will be notified of acceptance by March 11, 1994. Camera-ready copies are due not later than April 22, 1994.

Papers that use technology presented at a previous COMPASS conference are eligible for a special award. Papers of exceptional quality and appropriate subject matter are eligible for inclusion in a special issue of the Journal of High Integrity Systems or the Journal of Computer Security.

Limited financial assistance will be available for student authors.

PROGRAM COMMITTEE

Paul Ammann, George Mason Univ. (USA) John Marciniak, CTA (USA)

George Dinolt, Loral (USA) John McDermid, York Univ (UK)

Jan Filsinger, Booz-Allen Hamilton (USA) Jon Millen, Mitre (USA)

Virgil Gligor, Univ. of Maryland (USA) John McHugh, Portland State U. (USA)

Li Gong, SRI (USA) David Parnas, McMaster Univ. (Canada) Connie Heitmeyer, Naval Res. Lab. (USA) John Rushby, SRI (USA)

Jeremy Jacob, York Univ. (UK) Ravi Sandhu, George Mason Univ. (USA)

Carl Landwehr, Naval Res. Lab. (USA) Jeannette Wing, Carn. Mellon U. (USA)

Teresa Lunt, SRI (USA)

FOR FURTHER INFORMATION CONCERNING THE SYMPOSIUM, CONTACT:

Jan Filsinger, General Co-Chair John McLean, Program Chair Booz-Allen Hamilton, Inc Naval Research Laboratory

8283 Greensboro Dr. Code 5543

McLean, VA 22102 Washington, DC 20375 Tel: (703) 902-5302 Tel: (202)767-3852

Fax: (703) 902-3131 Fax: (202) 404-7942

filsing@itd.nrl.navy.mil mclean@itd.nrl.navy.mil



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 3

Thu 9 September 1993

Contents

Robot Disarms Man

David Fowler

The risks of Naive Users

Amos Shapir

The first programming errors

Jon Jacky

Offshore Data Havens

John R. Bruni

Re: The risks of CERT teams vs we all know

Jeff Schiller

Frederick Roeber

Re: Lost Crime Stats

Rodney Boyd

Into the void at the supermarket

Andrew Klossner

Re: What Constitutes an Exhaustive Attack?

A. Padgett Peterson

Fixing what's known to be broken

Tom Lane

Caller ID Blocking and 911

Monty Solomon

Bank mailing problem

Lauren Weinstein

Technology export curbs

Mich Kabay

Re: Security holes and risks of software like Sendmail

Marcus J Ranum

CfP: 1994 Z User Meeting Announcement

Jonathan Bowen

Call for Papers, Decision Science Conference

ACSLHL

Info on RISKS (comp.risks)

Robot Disarms Man

David Fowler <fowler@oes.ca.gov> Sat, 4 Sep 93 00:10:18 PDT

GREENBELT, Md. (AP)

Police used a 3-foot, 480-pound robot to disarm a man who allegedly shotgunned his girlfriend to death and barricaded himself inside their apartment. Prince George's County authorities sent the remote-controlled robot into the apartment Thursday after police were unable in a five-hour standoff to persuade Craig Smith, 22, to surrender. Smith fatally shot his live-in girlfriend Cynthia Wilkinson, 24, and sexually assaulted an unidentified woman who was a friend of Wilkinson's, police said. The woman jumped out a window of the second-story apartment and ran to a neighbor's home to call police.

After negotiations with Wilkinson broke off, police borrowed a robot that the fire department uses to dismantle suspected explosive devices, said Sgt. Alan Day, a police department spokesman. Transmitting the scene by a video camera, the robot at the direction of a fire department technician opened a closet door. Wilkinson could be seen hiding under a pile of clothes and the robot's mechanical claws reached out and pulled them away.

When Smith grabbed the clothes back from the robot and began to cover himself up again, the robot fired a high-pressure water gun to knock the shotgun out of Smith's hands and disorient him, said a police spokesman, Cpl. Keith Evans. Police rushed in and arrested Smith.

The Prince George's County Fire Department bought the robot known as Remote Mobile Investigator-9 RMI-9 for short seven years ago for \$45,000. Capt. Victor Stagnaro, a fire department spokesman, said it was the first time the local police had used RMI-9 to catch a suspect.

Smith was charged with first-degree murder and sexual assault. Evans said that Wilkinson and Smith argued Wednesday night after she apparently told him she wanted to end their relationship. The dispute resumed Thursday morning, and Smith shot Wilkinson while they argued, Evans said.

[Sept. 3, 1993 The Associated Press]

The risks of Naive Users

Amos Shapir <amos@cs.huji.ac.il>
7 Sep 1993 17:45:10 +0300

The following two articles were posted on a local BBS of a company I work for:

. 93/09/02 12:06 Entrance of children to our building. Following an incident which occurred last Tuesday evening (an employee's child switched off the UPS main electricity switch of one of the floors), we recommend that children not be left unattended in any part of the building.

The best advice is to stay with the children in the lobby where 'dangerous attractions' are minimal.

We have taken precautions to avoid recurrence of similar incidents by installing special locks on the electricity cabinets.

. 93/09/02 15:00 To those who suffered from the UPS fall

I apologize for my son, he's 20 month old, yet he needed less than 20 second on the floor to break the UPS down...

I checked the said UPS switch -- it's an emergency-shutdown type: big, red, and located near the bottom of the control panel. In short, conspicuous enough to be located quickly in an emergency -- or at any time by a two-year-old kid...

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp. Science. Givat-Ram, Jerusalem 91904, Israel, Tel: +972 2 585706 amos@cs.huji.ac.il

The first programming errors

Jon Jacky <jon@violin1.radonc.washington.edu> Tue, 7 Sep 93 21:48:36 -0700

There is an interesting story in THE SCIENCES, July/August 1993: "The Discovery of Debugging," by Brian Hayes, pps. 10 -- 13.

It describes experiences programming EDSAC, which the story says was the the first true stored program computer, at Cambridge in 1949.

EDSAC's first three programs -- which calculated lists of squares and prime numbers -- worked correctly the first time they were run! This was no mean accomplishment, in view of EDSAC's instruction set and the very rudimentary programming tools available.

After that, it got difficult. While cleaning his office in 1979, EDSAC designer Maurice Wilkes came upon a thirty year old punched tape which contained an early version of a program for calculating a table of values for Airy's integral. Wilkes gave a copy to Martin Campbell-Kelly, who studied it using an EDSAC simulator.

The 126 line program contained 20 errors! Most were trivial typos or logical errors, but one quite subtle error merely reduced precision in the fifth decimal place.

The story quotes from a memoir by Wilkes, who recalls the exact moment when "the realization came over me with full force that a good part of the remainder of my life was going to be spent finding errors in my own programs."

The SCIENCES story cites an article by Martin Campbell-Kelly in ANNALS OF THE HISTORY OF COMPUTING 14(4) 1992 and Maurice Wilkes' book MEMOIRS

OF A COMPUTER PIONEER.

- Jon Jacky, Department of Radiation Oncology, U. of Washington, Seattle

Offshore Data Havens

<John_R_Bruni@cup.portal.com>
Sun, 5 Sep 93 16:00:59 PDT

As a reader of RISKS who combines his vocation, journalism, with his avocation, computers, I'm writing in with a request. In the course of working on an assignment for one of the TV networks, I came across references to "offshore data havens." These are data networks, alleged to be in the formative process, which will glean data by means fair and foul from the world's legitimate data bases. The implication is that formerly confidential information, be it about individuals, corporations or governments, would seep across networks. The information would then be available, at a price, to anyone who wanted it.

My questions are:

- * Are "offshore data havens" actually being formed, and if so, where?
- * What are the inherent problems that come to mind? Don't be afraid to state the obvious; television audiences aren't experts in this area.

I'd love to see this become a topic for discussion on RISKS, but would also appreciate (with thanks in advance) any responses sent to me directly.

john_bruni@cup.portal.com

★ Re: The risks of CERT teams vs we all know (Cohen, RISKS-15.02)

Jeffrey I. Schiller <jis@mit.edu> Wed, 8 Sep 93 01:19:15 -0400

Let's go back and review history (briefly). The CERT teams, beginning with the original CERT at CMU, were a reaction to the now infamous Morris Worm of 1988. The folks who "solved" the worm problem by disassembling the worm and generating patches for the network community, in a matter of hours, were the university people, both staff and students.

Then, we had source code.

Today vendors are more and more making their source code unavailable, or too expensive, or available only under untenable terms(1). Fewer of us university people now have source code for contemporary systems. Yet the crackers out there have all the source code they can steal, which is quite a collection. I know, I saw it.

The network is as vulnerable today as it was in 1988... We'll see what happens the next time!

-Jeff

[1] Terms for example that prohibit students from having access.

★ Re: Risks of CERT teams (Cohen, RISKS-15.02)

Frederick Roeber <roeber@vxcrna.cern.ch> Wed, 8 Sep 1993 11:02:45 GMT

- > The problem with restricting information to CERT teams, etc. is that this:
- > 1 creates a techno-elite
- > 2 limits distribution far too much

And in any case, I don't think it works. A couple years ago, I was handed the job of running a cluster of machines at Caltech. Through various connections (Caltech, JPL, CERN, the HEP community, etc.) I ended up on many public and private mailing lists for security information, without even trying. Usually I'd receive a half-dozen slightly different copies of the same alert, before the sanitized CERT version went out. (This was useful for gauging the severity: if I only received a couple pre-CERT notes, I could probably defer the problem; if I received ten, I had to act.)

I think the restrictions the various Response Teams give themselves serve only to allow them to tell themselves -- and more importantly, their bureaucrats and lawyers -- "We're doing everything possible to limit the spread of dangerous knowledge." Whether their efforts in this direction accomplish anything or not is another question.

★ Re: Lost Crime Stats (Fernandes, RISKS-15.02)

Rodney Boyd <rodney@sq.sq.com> Wed, 8 Sep 93 16:08:45 GMT

According to the Globe and Mail (last Saturday, I think), the discrepancy arose because the police counted individual offenses, whereas StatsCan counted "incidents", which could encompass several offenses (e.g., a rape could result in charges of assault, sexual assault, use of a weapon, etc.).

--Rodney

Into the void at the supermarket

Andrew Klossner <andrew@frip.wv.tek.com> Tue, 7 Sep 93 13:27:02 PDT

While paying for groceries at a "pack the bags yourself" discount supermarket, I presented a chit for a \$15 credit, obtained when I returned several bags of soda cans. The cashier punched the cash register, and it stopped with an alert condition. It seems that "manager approval" is required whenever a

credit of more than \$5 is entered. At this store, the managers have long since tired of dealing with these alerts, so they have issued manager-only cash register override keys to all cashiers.

The cashier inserted and twisted a key, and the machine began to void out the entire \$100 transaction, item by item.

```
cat food, -$0.29
cat food, -$0.29
```

The cashier shrieked for help, but it was not to be had; the manager trainee on duty that Labor Day didn't know anything more than she did. After a minute or so, the cash register finished up and displayed

balance: \$0.00

The young lady turned to me and explained that she would have to pass every item over the scanner again. Unpack forty cans of cat food and fifty jars of baby food? I explained that this option was not available to her, and that she had needed to devise another solution.

She proceeded to phony up a set of transactions to create a balance identical to the one I'd had before the disaster. Her arithmetic was none too good, so she adjusted it by entering fictitious coupon discounts.

As I paid (the correct amount), she explained that there are *two* keys -- the "manager" key and the "professional" key. The latter is used only to turn on the cash register in the morning, and to void out an entire transaction. There is a single lock on the register, into which either key is inserted. The two keys are hard to distinguish from each other. And store management keeps them on a single keyring for ease of access.

(This same store also allows forklifts in the aisles during business hours, with employees riding the fork in violation of OSHA rules. And they are building a database of individual purchasing habits. It's a wellspring of RISK examples.)

-=- Andrew Klossner (andrew@frip.wv.tek.com)

Re: What Constitutes an Exhaustive Attack? (Murray, RISKS-15.02)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Tue, 7 Sep 93 13:19:21 -0400

>The cost of an exhaustive attack is an interesting number. It gives us an >upper bound for the cost of efficient attacks. However, it is never, itself, >an efficient attack.

What has bothered me for some time about Clipper/Capstone/SkipJack is exactly this question and the concern that what might be an exhaustive to some might not be what the user would think.

Consider the possibility that every person in the United States were issued a SkipJack key - better, suppose that every possible ZIP code in the United States were issued a key (10^9 as opposed to approx. 2.5*10^8 women, men, and children). Next suppose that every key issued were known (not WHO they were issued to, just WHICH had been issued). An exhaustive attack is now 10^9 trials with average success in 5*10^8 trials. At a 40 MHZ rate (common for DSPs) this would take well under a minute for an exhaustive search.

No trapdoors, backdoors, or weak keys. Just a database of all issued keys. In the sixties, a thief who wanted your GM car often did not have YOUR key, they had ALL the keys (on a ring about six inches in diameter - typically took about five minutes to find the right one).

The disclaimer here is usually one of random seeds etc but does anyone really think that every key is going to have a unique random seed? Or is it more likely that the two agents will each contribute their 80 bit piece and then a few thousand keys run off. And that the first (or last) from each batch along with the count might be for some nameless agency?

My belief is that the SkipJack algorithm is every bit as strong as everyone has said it will be. The question will it really take an exhaustive attack or will there be a "black bag" attack possible that will stem from the key generation process. Creative accounting at work.

Padgett

ps I believe in Clipper/Capstone/SkipJack & if the price is within reason will be one of the first to use it. Most people do not care if our government can listen in. Just no surprises, Teapot Domes, or fingerscrossed promises please.

Fixing what's known to be broken (Re: RISKS of elaborating on...)

Tom Lane <tgl@netcom.com> Sat, 28 Aug 93 19:58:25 -0700

jhudson@legent.com writes:

- > Now that 3 children have died and 13 more spent time in hospitals, local
- > organizations are distributing safety bars for windows.

This example reminded me of an old saying in the architectural and building trades: "Building codes are written in blood." Every requirement that exists in modern building codes was created to prevent a repeat of previous deaths.

Not that we should feel complacent, but the difficulty is hardly limited to software development. Taking shortcuts is a time-honored activity, and when it works it has clear benefits: there's no value in making a beam 10 times stronger than it needs to be, while there's lots of value in building a house affordably. The trick is to learn the *appropriate* safety factor. Neither safety-be-damned nor safety-at-ANY-cost is a workable approach. But probing the margin of what's safe tends to lead to accidents. As long as foresight is

not 20-20, there's no way around this.

Petroski's book "To Engineer is Human" is an excellent discussion of the technical and moral dilemmas involved here. Required reading for RISKS folk.

Tom Lane

Caller ID Blocking and 911

Monty Solomon <roscom!monty@Think.COM> Fri, 3 Sep 93 15:00:59 -0400

The following is an excerpt from the "Caller ID And Blocking Fact Sheet" I received from New England Telephone.

How Does Line Blocking Work With Emergency Calls?

If you have Line Blocking and an emergency service provider has

Caller ID, the provider will NOT receive your number UNLESS you

unblock your number by pressing *67 (dial 1167 on a rotary/pulse
phone) before you call '911' or other seven digit emergency numbers.

Line Blocking and Per-Call Blocking pertain to Caller ID only. Call Trace and Call Return are unaffected by either Line Blocking or Per-Call Blocking.

Monty Solomon / PO Box 2486 / Framingham, MA 01701-0405 # monty%roscom@think.com

[I have a huge collection of messages on blocking, dialing 1, *67, and related topics. I think we have peaked on those discussions, so I'll call a halt for a while. Thanks to all of you who sent in contributions on those topics. PGN]

★ Re: Bank mailing problem (Wood, RISKS-14.85)

Lauren Weinstein < lauren@vortex.com> Fri, 27 Aug 93 12:49 PDT

Kenneth Wood reported the saga of a bank that mailed letters to its 2000 wealthiest customers, all addressed to "Rich Bastard", thanks to a careless programmer.

It's worth noting that if the bank had given the mailing even a cursory check before dropping it into the mail stream, the odds are that the mistake would have been noticed and the mailing aborted. Of course, one can't expect a bank to personally inspect every envelope that churns out of their automated systems. But it would seem that with a relatively small mailing of such importance (dealing with your biggest customers) a little extra checking would have been a good investment!

The RISK is putting total faith in the system, of course.

--Lauren--

Technology export curbs

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 27 Aug 93 15:05:53 EDT

From Washington Post newswire 08/27

U.S. Acts to Ease Export Controls On Computers; Industry Officials Say Proposed Standard Falls Far Short of Need By Peter Behr, Washington Post Staff Writer

"The Clinton administration moved yesterday to ease Cold War-era controls on exports of high-powered U.S. computers to the former Soviet Bloc and other countries, fulfilling a campaign promise President Clinton made to the Silicon Valley executives who supported him last year."

The article continues with comments on the lost sales caused by Cold War restrictions on computer exports. The new Commerce Decision rules allow export of microprocessors rated at 67 Mops (million operations per second), a big boost from the previous limit of 12 Mops. However, multiprocessor units are still on the forbidden list.

Sales to the former Soviet Union are still subject to approval by COCOM, the Coordinating Committe for Multilateral Export Controls. Apparently some members of COCOM--Germany, in particular--are trying to link relaxation of computer export restrictions with relaxation of telecommunications gear.

It will be interesting to see if the long-standing assumption that export restrictions prevent the distribution of technology to the interdicted nations. My reading of the DES-restriction debacle is that export controls on high tech are a farce. The U.S. restrictions hurt U.S. manufacturers and are a boon for everyone else.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Re: Security holes and risks of software like Sendmail

<mjr@TIS.COM> Fri, 27 Aug 93 15:22:58 -0400

The only conclusion I seem to be able to draw from problems like the sendmail DEBUG hole is that more care needs to be spent designing software so that bugs in security-critical programs CANNOT compomise the system.

Mailers are inherently complicated things, that require privileges in order to work. It seems to me that in designing a complex program that

requires privileges, the complex part and the privileged part should be separated. The privileged part should be simple enough that its function can be verified in a couple of minutes of code-browsing with a cup of cappucino. The complex part can be as convoluted and gnarly as you wish, and can have all the debug options its complexity requires.

A good example of this design philosophy is anonymous FTP. There was a pretty nasty bug recently described in the wustl ftpd, a popular implementation that is widely used. Any user on the network could get root access to a system running that version of ftpd. How can this happen? Because ftpds are complicated and do lots of stuff (especially the wustl one, which is extremely "feature heavy") - they also require privs in order to work right. This is a deadly combination. You'll find it wherever there are consistent security problems. A lateral thinking approach to FTP is to configure ftpd the way we do at TIS: you do the chroot and setuid before ftpd is even invoked.

Ideally, the worst the complex code can do to you is give you a core dump. Ideally, the critical code should be a page or 2 of clear, straightforward operations. If you have to comment your security critical code, perhaps it's too complex. ;)

mjr.

✓ CfP: 1994 Z User Meeting Announcement

Jonathan Bowen <Jonathan.Bowen@comlab.ox.ac.uk> Sat, 28 Aug 93 15:47:38 BST

Notice of Meeting and Call for Papers
8th Z User Meeting - ZUM'94
Organized by the Z User Group in association with BCS FACS
29-30th June 1994
St. John's College, University of Cambridge, UK

Program committee:

Rosalind Barden, Logica, Cambridge Jonathan Jacky, Univ. of Washington, USA

Jonathan Bowen, Oxford Univ. Peter Lupton, IBM Hursley Elspeth Cusack, BT John McDermid, York University

Neville Dean, Anglia Polytechnic Univ. Sylvio Meira, Univ. of Pernambuco, Brazil

David Duce, Rutherford Appleton Lab. John Nicholls, Oxford Univ.

Anthony Hall, Praxis plc Gordon Rose, Univ. Queensland, Australia

Brian Hepworth, British Aerospace Chris Sennett, DRA Malvern
Howard Haughton, Lloyd's Register Sam Valentine, Univ. of Brighton
Mike Hinchey, Univ. of Cambridge Jim Woodcock, Oxford Univ.

Darrell Ince, Open Univ. John Wordsworth, IBM Hursley

The committee of the Z User Group invites the submission of papers related to the interests of users of the formal notation Z. Sessions on the following themes are planned, and papers on these topics are especially encouraged:

* Industrial experiences

- * Application of Z to safety-critical systems
- * Projects and processes for formal methods organizational issues
- * Z and concurrency
- * Educational issues (an extra half-day session)

Papers for presentation and publication will be reviewed and selected by the program committee. The timetable for submitted papers is as follows:

Submission of draft paper: 1st October 1993

Notification of acceptance: 30th November 1993

Final copy for Proceedings: 31st January 1994

Z User Meeting in Cambridge: 29-30th June 1994

A maximum limit of 20 pages is requested. Industrial contributors may submit extended abstracts if they prefer. Please include four copies of your submission and indicate if you wish your paper to be considered for one of the special themes. The following invited speakers are planned:

David Garlan, Carnegie-Mellon University, USA: Z and education Mike Gordon, University of Cambridge, UK: Z and HOL

Leslie Lamport, DEC Systems Research Center, USA: Z and concurrency

Jim Woodcock, Oxford University, UK: Z and MoD 00-56 Robert Worden, Chairman of Logica Cambridge, UK: Z and industry Maurice V. Wilkes, Olivetti Research (Emeritus Professor, University of Cambridge): After dinner speaker on the occasion of the 45th anniversary of the EDSAC meeting (first European computer conference) held in Cambridge, June 1949, and hosted by him.

The meeting will be sponsored by BT, Logica and Praxis and is supported by the UK BCS FACS group the European ESPRIT ProCoS-WG (8694) Working Group.

General enquiries may be directed to:

Jonathan Bowen (Conference Chair)

Oxford University Computing Laboratory, 11 Keble Road, Oxford OX1 3QD, UK

Email: Jonathan.Bowen@comlab.ox.ac.uk Tel: +44-865-272574, Fax: +44-865-273839

Submitted papers and extended abstracts should be sent to:

Anthony Hall (Programme Chair)

Praxis Systems plc, 20 Manvers Street, Bath BA1 1PX, UK.

Email: jah@praxis.co.uk

Tel: +44-225-444700, Fax: +44-225-465205

Proposals for tutorials, tool demonstrations, publishers' stands, and requests for information concerning local arrangements should be sent to:

Mike Hinchey (Tutorial Chair)

University of Cambridge, Computer Laboratory

New Museums Site, Pembroke Street, Cambridge CB2 3QG, UK

Email: Michael.Hinchey@cl.cam.ac.uk

Tel: +44-223-334419, Fax: +44-223-334678

Until beginning of October 1993 at DEC Systems Research Center,

Palo Alto, California, USA, Email: hinchey@src.dec.com

A special session on Educational Issues relating to Formal Methods (Z

in particular) is being organized for the Friday morning (1 July 1994) after the main Z User Meeting 1994 to be held in Cambridge (29 and 30 June 1994). For further information, please contact:

Neville Dean (Education Session Organizer)

Applied Sciences, Anglia Polytechnic University, Cambridge CB1 1PT, UK

Email: CDEAN@vaxa.anglia-polytechnic.ac.uk

Tel: +44-223-352992 ext 2329, Fax: +44-223-352979

Call for Papers, Decision Science Conference

<aCSLHL@vaxc.hofstra.edu> Tue, 07 Sep 1993 17:31:43 -0400 (EDT)

Subscribers to RISKS may be interested in attending and/or presenting a paper at the 1994 Annual Meeting of the Northeast Decision Science Conference, April 6-8, at the Sheraton Hotel and Conference Center in Portsmouth, New Hamshire. The conference has a Business Law/Business Ethics track which last year featured papers on the implications of the Americans with Disabilities Act for ATM managers, and the legal implications of Expert System use.

Other tracks include:

Accounting
Curriculum and Studies
Environmental Management
Finance and Real Estate
Human Resource Management
International Business
Management Science
Marketing
MIS/DSS/AI
Microcomputing
Organization, Theory, Policy and Behavior
Operations Management
Quality/Productivity
Service Management
Statistical Theory & Applications

Papers presented are also published in the conference proceedings. All papers must be double spaced. Authors must submit one copy plus three additional copies for each track for which the paper is to be considered. Papers should not exceed 20 pages in length. Each copy of the paper should have two title pages. The first should have both the title and author information (including mailing address); the second should have only the title. Each submission should include a 3" X 5" card with the following data:

- 1. Author(s)
- 2. Affiliation
- 3. Address(es)
- 4. Office and Home Phone Numbers
- 5. Submission Title
- 6. Appropriate Track(s)

Each submission should also include a stamped, self-addressed postcard with the author(s) name and the title of the submission for acknowledgement of receipt by the Program Chairperson.

Papers must be received no later than October 3, 1993. Notifications of acceptance will be mailed by December 1, 1993. Accepted papers must be typed in final condensed and camera-ready form and returned to the Proceedings Editor by January 5, 1994. Specific instructions will be mailed to the authors with the acceptance letters.

Submissions are to be sent to:

Dan Reid 1994 NEDSI Program Chairperson Whittemore School of Business and Economics University of New Hampshire Durham, NH 03824 (603) 862-3382

The Sheraton Portsmouth Hotel and Conference Center has provided a limited number of rooms at the rate of \$89-94/night (single) and \$99-104/night (double), plus tax. (For reservations call (603) 431-2300 and state that you are attending the NEDSI Meeting). Other questions, contact chair.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 4

Friday 10 September 1993

Contents

<u>EuroDigital</u>

Brian Randell

- Brussels Branch Of BNP Hit By Computer Fraud
- Screen savers hide what's running below them Alan Munn
- Where should we look for risks?

Steve Talbott

- Re: Security holes and risks of software ... Geoffrey H. Cooper John Carr
- Re: "Offshore Data Havens"

Fred Baube

Gary Preckshot

Re: The risks of Naive Users

Mark Brader

- Re: More Gripen Griping **Mark Stalzer**
- Info on RISKS (comp.risks)

EuroDigital

<Brian.Randell@newcastle.ac.uk> Thu, 9 Sep 1993 18:10:41 +0100

The attached article about a new digital phone service, about to be launched in the UK, is from the Monday, Sept 6, 1993, issue of The Independent. Also in this issue was a two page advertisement for the new service - the text of this is also attached. My understanding is that the new equipment produces emissions that have characteristics that were not considered when the regulations and guidelines (under which existing devices such as hearing aids were designed) were laid down. If this is right, then the statement by the providers of the new service that the problems are the responsibility of the manufacturers of such devices would seem to be highly questionable. I await

with interest RISKs readers' reactions to the article (and the advertisement).

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

========

PHONES - THREAT TO HEARING AID USERS Mary Fagan

More than two million people who are deaf or hard of hearing face distress and discomfort with the launch this autumn of new digital mobile telephone equipment that interferes with hearing aids, according to the Royal National Institute for the Deaf. The telephones could also cause interference if used close to computer screens, and there is speculation that they could cause problems with other electronic equipment.

Last week, Vodafone launched a digital mobile telephone service and Mercury's One-2-One digital service will be onstream within weeks. Cellnet hopes to start a commercial service next year.

The new telephones send pulses of radio signal rather than the continuous signal sent by existing analogue cellular telephones. According to the RNID, when these pulsed signals are transmitted close to audio and video equipment they are picked up in wiring, causing interference.

Mike Martin, the RNID's chief scientist, said hearing aid users standing up to six feet from a handheld mobile phone could be affected. More powerful car phones could affect pedestrians.

The telephones can cause people wearing hearing aids to hear a noise like a bee buzzing. It can drown out other sound and cause pain and considerable distress, a spokesman for the RNID said.

Cellnet and Vodafone admit there can be problems with hearing aids and computer screens. But the companies say the problem is with the telephones - which they do not manufacture - and with the equipment affected by them.

A spokesman for Vodafone said that the real problem was the standard of hearing aids. In Germany, where there has been most experience with digital telephony, no problems have been experienced.

A spokeswoman for Mercury One-2-One said that as the telephones used on One-2-One were very low-power, only equipment very close by could be affected.

(Advt.) LIBERTE'

The Freedom to make a call in total security

We have given you freedom. We have created a secure tomorrow for businessmen and travellers both here and in Europe. New frontiers beckon. Vodafone proudly announces EuroDigital. The most advanced and most secure mobile phone

network. So sophisticated that it can even be used to make and receive calls in Europe in total security. EuroDigital represents a revolution in mobile phone technology. A superior digital system that provides a top quality service. A quality that doesn't falter, that doesn't break up. Line rental is 21.50 per month. UK call charges 25p per minute peak, 10p off peak. Only Vodafone can offer this. Liberate yourself. Enjoy freedom of speech and security. Rise above the rest. Call free, 0500 123 123 and ask for more information. All prices are recommended and are exclusive of V.A.T.

VODAFONE EuroDigital

Brussels Branch Of BNP Hit By Computer Fraud

<jxm@engin.umich.edu>
Thu, 9 Sep 93 14:41:22 -0400

Brussels, Belgium, September 8, 1993 (NB) -- The Belgian office of Banque Nationale du Paris (BNP) has admitted it was the victim of a major computer fraud in June of this year, according to Belgian press sources. The AFP news agency reports that a total of BFr 245 million was taken in the computer fraud, although bank officials have now recovered the money and Police are holding two suspects. The two fraudsters used their direct computer access facilities to request debits from BNP accounts and switch the proceeds into their own bank accounts with other banks. According to BNP sources, auditors picked up the fraud when they carried out a routine series of checks on inter-bank transactions in June.

As soon as the fraud was discovered, the third party banks were contacted and the money recovered. As a result of the fraud, BNP is carrying out an internal inquiry into how the frauds occurred and whether its security systems can be beefed up to prevent a recurrence.

Screen savers hide what's running below them

Alan Munn <ENGALAN@MIZZOU1.missouri.edu> Fri, 10 Sep 93 15:18:40 CDT

I discovered (the hard way) that screen savers can be dangerous if you don't know what's running underneath them. Normally when you pop a disk into a Mac with a screen saver running, it stops the screen saver and presents you with whatever is running at the time. It so happened that when I stuck my disk into our Computer support person's machine, she had been running Apple's Disk Copy program, which once you get it started blindly accepts disks and makes a copy of the resident disk image. This is handy if you have lots of disks to make, but was fatal in my case, since my disk was completely erased. I did have copies on my hard disk, but...

The moral of the story is don't stick your disk into a machine if you don't know what it's doing.

Alan Munn <amunn@mizzou1.missouri.edu>
Dept. of English University of Missouri, Columbia MO 65211

P.S. On a lighter note, windows without screens are also a risk. I swatted at a bug that came flying at me last night and my glasses flew out the window onto the grass (luckily) two stories below. Of course I couldn't look for them until I found them, so I had to call campus police to help out.

Where should we look for risks?

Steve Talbott <stevet@ora.com> Thu, 9 Sep 1993 15:52:05 EDT

I was gratified to receive some 30 responses to my post "worrying about online education" (RISKS-14.86). Most were sympathetic, and the majority of those that were critical still made a point of saying that the subject is well worth discussing in forums like RISKS.

That poses a problem for moderators, however, for I have to admit that the tendency of such discussions is almost always to violate the (desirable) standards enforced by the moderator. Looking at the division among USENET discussion groups between those that "get real work done" and those that pursue "philosophy," one is tempted to conclude that it's in the very nature of the net to disallow the sensitive and constructive exploration of complex or deep issues. The system is more suited for what we like to call the exchange of "information." Perhaps that is one of the risks!

Well, I don't have any particular solution to offer. I find myself unable to tolerate the philosophical groups, but am still driven to pursue issues that seem slightly out of place in the more business-like groups. One thing this dilemma has done, however, is to push me toward the formulation of the most concise (business-like!) statement I could manage regarding the question, "Where should we look for technological risks?" To offer a parallel: anyone speaking about the effects of television upon society would probably no longer be content merely to point at a set of good (or bad) TV programs. There are deeper questions that require us to penetrate the medium itself, as well as our own natures.

Perhaps the following 4 paragraphs--representing my attempt to answer the question voiced above--will interest some members of this group.

Obviously, such a statement can only be a preface to particular studies, but it seems to me worth keeping in mind. As always, I welcome critical comment.

Steve Talbott stevet@ora.com

In assessing the complex "symbiosis" between man and machine, it will hardly do to look for external cause and effect. Every contrivance, from

the plow to the hydrogen bomb, expresses something within *us*. If we extend ourselves in our mechanical tools, we also meet ourselves in them.

At the same time, just as the corporation seems to gain a life and tendency of its own, independent of its employees, so too the machine can become almost willful in its reaction upon its creators. "To someone who possesses only a hammer, everything begins to look like a nail." It is important, nevertheless, to recognize ourselves in this willfulness, even if doing so requires a bit of painful psychological excavation.

The machine's double existence as an expression of the human being and as an independent force is most fully realized in the computer. Just consider those several disciplines--psychology, linguistics, philosophy, artificial intelligence--whose natural confluence has given us the remarkable developments in cognitive science. Here the pressing question is not so much, "How are computers expressions of ourselves?" as it is the much balder, "Are computers selves?" We who produce such devices cannot escape our own most intimate responsibility for the planet's rapidly crystallizing, electromechanical nimbus, nor can we escape the prospect of its increasing--and potentially threatening--independence and self-will.

All this is to say, in a nutshell, that if we cannot point to any simple determination of society by machines, neither can we claim straightforward human control of the effects of those machines. We and our mechanical offspring are bound together in an increasingly tight weave. This has one clear implication: to substantially modify the larger pattern--rather than simply be carried along by it--requires profound analysis of things not immediately evident, and a difficult effort to change things not easily changed. If it is only by a certain self-awareness and an inner adjustment that I can restrict the hammer in my hands to its proper role, I must multiply the effort a millionfold when dealing with a vastly more complex technology--one endowed in a much more powerful sense with its own willful tendencies.

Steve Talbott stevet@ora.com

Copyright 1993 Stephen L. Talbott. You may freely redistribute these remarks on a not-for-profit basis so long as this notice and the remarks themselves are left fully intact and unedited.

★ Re: Security holes and risks of software ... (Ranum, RISKS-15.03)

Geoffrey H. Cooper <geof@aurora.com> Fri, 10 Sep 93 14:31:07 PDT

> ...It seems to me that in designing a complex program that requires > privileges, the complex part and the privileged part should be separated...

I agree with this statement, but find another conclusion/RISK. This is the risk of having security mechanisms that are too cumbersome to be used easily.

Following the example given, classical UNIX provides only the setuid mechanism for increasing the access of a program, and setuid always applies to an entire program. Thus, if a program must run partially as root, the only way to avoid having it ALL run as root is to divide it up into communicating processes. Depending on the application, this is not always easy to do.

If you want security, you have to make it easy to be secure. For example, if a setuid program had to explicitly enable and disable the setuid access (running otherwise as the user who invoked it), the body of code that needed to be carefully checked to verify security would be significantly diminished; a loophole in another part of the program could not compromise the entire system's security.

- Geof

★ Re: Security holes and risks of software (Ranum, RISKS-15.03)

John Carr <jfc@Athena.MIT.EDU> Fri, 10 Sep 1993 19:52:05 EDT

>Ideally, the worst the complex code can do to you is give you a core dump

Back in 1988 I was writing a program which connected to a finger server. I knew enough about UNIX at the time to go to the real documentation: the source code for fingerd. I noticed a fixed size buffer, and verified that sending a long string would make fingerd crash. Just a core dump, right? And fingerd is restarted by inetd for each new request, so there is no denial of service. I thought so, and didn't follow up.

A few months later everyone learned that there were worse side effects.

Think of a core dump as the best thing that can happen when your program goes wrong, not the worst. If you want a program to dump core under certain conditions, call abort(). Don't depend on memory corruption to do the job right.

--John Carr (jfc@athena.mit.edu)

[On the other hand, getting a system to dump core can be gold mine of information for a malicious attacker... P.]

★ Re: "Offshore Data Havens" (Bruni, RISKS-15.03)

F.Baube[tm] <flb@flb.optiplan.fi> Fri, 10 Sep 93 10:03:37 EET

Perhaps someone else has provided the reference, but there is a very well-written science fiction novel which explores vividly and in some detail the concept of "offshore data haven". This is "Islands in the Net", by Bruce Sterling, a well-known author in the "cyberpunk" genre.

The point of the book is that an international "black market" in information about individuals is inevitable and unstoppable.

I highly recommend the book. Don't let the foolish cover illustration put you off.

Fred Baube (tm) GU/MSFS/88 baube@optiplan.fi

★ Re- Off-shore data havens (Bruni, RISKS-15.03)

"Gary Preckshot" <gary_preckshot@lccmail.ocf.llnl.gov>
10 Sep 1993 13:23:48 U

The interesting to me about this report is the nuance of ownership of the data. Presumably the "legitimate owners" of the data are wroth since only they are allowed to sell, or otherwise profit from, our privacy. We're already embroiled in a continuing dispute over a restricted form of data termed "intellectual property" and we've been unable to resolve even relatively simple issues in that regard. So it's interesting to contemplate how one "owner" of data would proceed against some other "owner" of data for "stealing" the former's data. Whose name is on the data? Owner #1, owner #2, or your name, or my name? What risks are we running here? Possibly

- 1) Financial loss to owner #1
- 2) Financial loss to owner #2
- 3) Loss of privacy to third party
- 4) Onerous litigation that burdens everybody
- 5) Foolish laws passed by Congress

Given the noted ability of our courts to resolve current intellectual property imbroglios (microcode and program copyrights), a paraphrase of Mark Twain's comment is probably appropriate: no one's life or property is safe while court is in session. There are so many potential victims and litigants that circumscribing risks may defy our meager abilities. Maybe the best thing to do is just to ignore off-shore data havens, since the cures and the would-be doctors are all worse than the disease. And you can get the data for a price right now, anyway.

★ Re: The risks of Naive Users (Shapir, RISKS-15.03)

Mark Brader <msb@sq.com> Fri, 10 Sep 1993 16:56:00 -0400

- > I apologize for my son, he's 20 month old, yet he needed less than
- > 20 second on the floor to break the UPS down...

Anyone else reminded of this entry in the Jargon File?

:molly-guard: /mol'ee-gard/ [University of Illinois] n. A shield to prevent tripping of some {Big Red Switch} by clumsy or ignorant hands. Originally used of the plexiglass covers improvised for the BRS on an IBM 4341 after a programmer's toddler daughter (named Molly) frobbed it twice in one day. Later generalized to covers over stop/reset switches on disk drives and networking equipment.

Mark Brader ...the scariest words of the afternoon:

SoftQuad Inc., Toronto "Hey, don't worry, I've read all about utzoo!sq!msb, msb@sq.com doing this sort of thing!" -- Vernor Vinge

★ Re: More Gripen Griping

<stalzer@macaw.hrl.hac.com>
Thu, 9 Sep 93 14:32:58 PDT

Mary Shafer writes on Thu, 26 Aug 93 15:40:49 PDT (RISKS-14.89): >As far as I can tell, the real problem was control-surface rate limiting. >Cf. the YF-22 crash and the Space Shuttle ALT-5 multi-axis PIO. >

>I've flown a rate-limited configuration in a variable-stability Learjet >and it looked a lot the same, just before the safety trips gave the plane >back to the safety pilot.

My flight experience is minimal, but in a small plane the maximum rate at which control surfaces can be moved is limited only by the pilot's strength and desire not to damage the plane. More importantly, there is a direct connection between the position of the control surface and the stick. I believe this form of feedback exists even on large planes that have hydraulically assisted control surfaces. Apparently, in fly-by-wire aircraft, there may not be much of a correlation between the position of the stick and the control surfaces. What used to be a closed-loop control system is now more open-loop. The aviation community must have done some studies on how this lack of feedback can effect pilots, especially during critical situations (when a pilot reverts back to his or her most fundamental training). Or was it just assumed that pilots would adapt to the new ``user interface''? -- Mark

Mark Stalzer, Hughes Research Labs RL65, 3011 Malibu Canyon Rd, Malibu CA 90265 E-Mail: stalzer@macaw.hrl.hac.com Voice: 310-317-5581 FAX: 310-317-5483



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 5

Thu 30 September 1993

Contents

An oxymoron?

Jim Horning

Unfriendly fire

Tim Steele via Jim Thompson

RISKS BY FAX

Lauren Weinstein

Risks of Flying Toasters?

Jim Griffith

Ilyushin Il-114 crash

Urban Fredriksson

Cancer Treatment Blunder

Brian Randell

RFI from phones (was "EuroDigital").

Mich Kabay

Fungible microprocessors

Mich Kabay

Re: Security holes and risks of software ...

A. Padgett Peterson

Josh Osborne

John Hascall

DCCA-4 Advance Program

Teresa Lunt

An oxymoron?

<horning@src.dec.com> Fri, 24 Sep 93 18:05:50 -0700

An announcement recently posted at an installation that shall remain nameless:

Subject: IMPORTANT: All machines will be down

ALL MACHINES WILL BE DOWN!

When: Saturday morning (9 to 13) September the 25th Why: Maintenance of the UPS (Uninterruptible Power Supply)

Unfriendly fire

Jim Thompson <jim@Tadpole.COM> 27 Sep 1993 13:41:14 GMT

>From our system administrator in the UK

Date: Mon, 27 Sep 93 11:28:00 BST From: tjfs@tadtec.co.uk (Tim Steele)

To: ttp@tadtec.co.uk

Subject: Macintosh Users Please Read

Last week we had another Mac SE catch fire. We were lucky that it was during the day and could be switched off quickly.

As a general principle, if you can switch your equipment off at night you should do so. Unix systems are a bother to shut down, and are normally designed to run 24 hours, so it's OK to leave them on.

Mac SE (and SE/30) users should consider this mandatory, as they have a known propensity to catch fire.

Thanks, Tim

RISKS BY FAX

Lauren Weinstein <lauren@vortex.com> Sun, 26 Sep 93 21:21 PDT

Please change the voice contact number for fax information to (818) 225-2800. The fax number should be changed to (818) 225-7203. We've moved. Thanks.

--Lauren--

✓ Risks of Flying Toasters?

Jim Griffith <griffith@fx.com> Thu, 30 Sep 93 13:29:23 PDT

Heard on the radio that Berkeley Software, the people who brought you the flying toaster screen saver, have filed a lawsuit against Del Rio of Canada ("Del Rio" probably misspelled - radio, remember?) regarding that company's new "Opus and Bill" screen saver. The screen saver in question features Our Favorite Penguin using a shotgun to blast, you guessed it, flying toasters. The lawsuit asks for a "cease and desist" order against the sale of the product.

Berkeley Software apparently tried to negotiate a settlement, and the lawsuit signifies that their efforts failed.

Jim

[Added LATER note, from Mark Brader: It was Delrina Corp. They lost the suit, and proposed to change to toasters with helicopter rotors. msb]

✓ Ilyushin Il-114 crash

Urban Fredriksson <urf@icl.se> Mon, 27 Sep 1993 18:31:08 GMT

The reason for the fatal crash of Ilyushin II-114 prototype regional turboprop was that the digital engine control system inadvertently commanded one propeller to feather just after take off on July 5:th. The pilots couldn't compensate for the resultant yaw. [Flight International 15 - 21 Sept 1993] -- Urban Fredriksson urf@icl.se

Cancer Treatment Blunder

<Brian.Randell@newcastle.ac.uk>
Thu, 30 Sep 1993 15:05:07 +0100

Today's Independent carries a front-page story headed:

"Cancer Blunder Will Cost Health Authority Millions", by Celia Hall and Jonathan Foster.

It is based on a report, by Dr Thelma Bates and Dr David Ash, commissioned by the relevant Health Authority into the accidental mistreatment of a large number of cancer patients at the North Staffordshire Royal Infirmary. Here are some quotes from the article:

"A Health Authority last night faced the prospect of finding millions of pounds from its patient budget to pay compensation after a mistake which led to more than a thousand people getting the wrong cancer treatment.

It is impossible to be sure how many of the patients have died because of the underdosages - but the number is likely to be in the tens rather than in the hundreds.

Details of the errors were disclosed after a clinical inquiry by senior radiologists who examined the cases of all 1045 patients who had radiation doses of up to 35% less than prescribed. Their report blamed human error by Margaret Grieveson, a physicist, who unnecessarily programmed a correction factor into the radiography computer in 1982."

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

 $http://catless.ncl.ac.uk/Risks/15.05.html [2011-06-11\ 12:03:17]$

RFI from phones (was "EuroDigital")

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 11 Sep 93 15:09:46 EDT

In RISKS 15(4) Brian.Randell@newcastle.ac.uk wrote about the radio-frequency interference (RFI) generated by new digital phones.

This issue raises serious security questions. Winn Schwartau of Inter.Pac has been writing about high-energy radio-frequency ("HERF guns") for years. Pulses of electro-magnetic radiation can hang or crash microprocessors from a distance. They can cause processing and memory errors. It now seems anyone will be able to buy a phone which emits high-energy radio-frequency pulses sufficient to interfere with the microprocessor in a modern hearing aid.

Would RISKS readers be on the lookout for the results of tests of the effects of such phones on microprocessors? A short time ago in RISKS we read about cellular phones causing motorized, computer-controlled scenery to shift about in one of Andrew Lloyd-Webbers's productions in London. I wonder what happens to a spreadsheet when one of these noisy phones goes off while we're busy trying to compute?

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

✗ Fungible microprocessors

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 11 Sep 93 15:10:20 EDT

A story delivered by CompuServe's Executive News Service newswires through my topic-filters into the "Security" in-box caught my eye yesterday afternoon:

"OTC 09/10 1606 Violent computer chip takeovers worry officials

SAN JOSE, Calif. (Sept. 10) UPI - The lucrative trade in computer chips has captured the attention of the state's street gangs, luring them to California's Silicon Valley where the armed takeover of supply warehouses has become a common occurrence, authorities said Friday."

The article includes an interview with Julius Finkelstein, deputy district attorney in charge of Santa Clara's High Tech Crime unit. Mr Finkelstein thinks that there is a trend towards violent robberies of computer processors in Silicon Valley because of the high demand for these chips. One of the reasons the chips are so lucrative on the gray market is that they have no serial numbers and cannot be traced to a stolen lot. The chips are as valuable as cocaine on a weight-for-weight basis, he said.

The most recent case occurred on Thursday, 9 Sept 93, when six thieves attacked Wyle Laboratory Inc. in Santa Clara in a well-planned, precise operation which netted thousands of dollars of Intel CPUs. Apparently the

thefts have reached one a month so far, with signs of worsening as criminal street gangs realize how low their risks are, either of capture, successful prosecution or sentencing.

CPU chips, like pennies but not dollar bills, are fungible. That is, they are indistinguishable and equivalent. When a manufacturer buys gray-market CPU chips, there is no way to identify them as stolen because there is no way to tell which chips came from where and how they got there.

How long will it be before this kind of RISK to workers and loss for manufacturers leads to a cryptographically-sound system for imposing serial numbers on microprocessors? In this case, a unique ID could not only save money, it could save some innocent person's life.

Could the chip manufacturers engrave a unique ID on their chips during the wafer stage using their normal electron-beam/resist/UV/acid production phase? Each chip in a wafer would have a sequence number, and each wafer might have a wafer number. For such ID to be effective in reducing the fungibility of microprocessors, each manufacturer would have to keep secure records of their products and where they shipped them, much as pharmaceutical manufacturers and many others do. Would such an engraved number be readable once the chip were encapsulated? Does anyone know if X-rays, for instance, could pick up the engraved numbers?

Another approach might be to integrate a readable serial number in the physical package in which the CPU is embedded. Perhaps a unique, IR-readable information could be molded into the plastic or epoxy-resin package using technology that has already been applied successfully to producing access-control cards. Other technology that might be applicable includes the Wiegand effect, where the orientation of ferromagnetic spicules in a plastic matrix produces a characteristic and individual response to a radio-frequency electromagnetic beam. Perhaps it would be wise for the industry to agree on some standards to make it easier to read such numbers using a simple, inexpensive technique.

How much would all this engraving and record-keeping cost? Surely the costs would ultimately be borne by consumers; therefore, individual companies may balk at identifiers because they could derive a short-term competitive edge by continuing to manufacture fungible chips. In the long run, however, if theft continues to increase, plants producing identical chips may become the preferred targets of chip thieves.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

★ Re: Security holes and risks of software ... (Ranum, RISKS-15.03)

> ...It seems to me that in designing a complex program that requires

> privileges, the complex part and the privileged part should be separated...

The interesting part is that for the first time we are approaching the point where true separation is possible. Not in a mainframe, nor in a UNIX machine but in the client-server network (not peer-peer though).

The problem is that the traditional architecture is a single-state machine and each operating condition is linked to every other condition. Security it built on top of what starts out as a single privileged user state.

Until now, the client-server relationship has been viewed simply as a collection of such single state machines (and a peer-peer network is). More and more we are starting to see security and integrity products (anti-virus NLMs were the first) that consider the synthesis of clients and servers as a multi-state machine with the clients unable to influence the server (well, clients could flood the net but this does not affect the server).

IMHO this changed world-view is going to cause the single greatest change in information security that we have ever seen. Networks will cease being "unsecurable" and become the only accepted means for protection of data.

Padgett

★ Re: Security holes and risks of software ... (Ranum, RISKS-15.03)

Josh Osborne <stripes@uunet.uu.net> Fri, 10 Sep 93 23:14:43 -0400

>Following the example given, classical UNIX provides only the setuid mechanism >for increasing the access of a program, and setuid always applies to an entire >program. Thus, if a program must run partially as root, the only way to avoid >having it ALL run as root is to divide it up into communicating processes.

Not true. A program may return from its effective uid to its real uid at any time (on BSD systems it may swap the euid & ruid, which isn't a great improvement - homework question, why?). I have a program that needs to use a raw socket to do its job, only root can get open a raw socket. Any uid can _use_ a raw socket. The very first thing my program does is open the raw socket (and check for errors). The very second thing it does is set the euid to the ruid. It does this before even parsing command line options (which anoys me, you can't get it to print the usage message if you don't run it as root, or set-uid it). If the program has a bug somewhere else in it that can be used as a security hole, the damage is limited to allowing an unprivileged user access to a raw socket. How bad is that? Well they can send almost anything onto the net with one, simulating connections from privileged ports, or other (normally near-by) hosts. If the site allows .rhost files it could be in for some trouble. It will take alot of programming effort to achieve this 'tho - an entire TCP/IP stack in user space, and a rlogin that uses it.

[...]

Re: Security holes and risks of software ...

```
<john@iastate.edu>
Fri, 10 Sep 93 23:13:31 -0500
```

mjr@tis.com (Marcus J. Ranum) writes:

- > ...It seems to me that in designing a complex program that requires
- > privileges, the complex part and the privileged part should be separated...

geof@aurora.com (Geoffrey H. Cooper) writes:

}I agree with this statement, but find another conclusion/RISK. This is the }risk of having security mechanisms that are too cumbersome to be used easily.

}Following the example given, classical UNIX provides only the setuid mechanism }for increasing the access of a program, and setuid always applies to an entire }program. Thus, if a program must run partially as root, the only way to avoid }having it ALL run as root is to divide it up into communicating processes.

Not true, but perhaps a good idea, just the same.

If you want security, you have to make it easy to be secure. For example, if a setuid program had to explicitly enable and disable the setuid access (running otherwise as the user who invoked it), the body of code that needed to be carefully checked to verify security would be significantly diminished; a loophole in another part of the program could not compromise the entire system's security.

Under BSDish flavors of Unix (at least), it is indeed possible to turn "setuid" on and off using the "setreuid()" call. Although, some network file systems can make it a little less straight forward than it might be...

```
/*
 * Do a fancy jig (dance around AFS & NFS)
 */
setreuid(0, pwd->pw_uid);
chdir(pwd->pw_dir);
setreuid(pwd->pw_uid, 0);
/*
 * can access files as user here
 */
if (!quiet) quiet = (access(qlog, F_OK) == 0);
if (Xflag) doXauth();
/*
 * back to root
 */
setreuid(0, 0);

From: John Carr <jfc@Athena.MIT.EDU>
>Ideally, the worst the complex code can do to you is give you a core dump
}[...the classic fingerd buffer overwrite...]
```

}[...the classic fingerd buffer overwrite...]
}A few months later everyone learned that there were worse side effects.
}
}Think of a core dump as the best thing that can happen when your program goes

}wrong, not the worst. If you want a program to dump core under certain
}conditions, call abort(). Don't depend on memory corruption to do the job
}right.

I think this illustrates that separating the complex part from the privileged part is more subtle than would appear at first blush. It does little good to have the privileged part carefully segregated into an easily understood module if the complex part can scribble all over it or its data.

John Hascall, Systems Software Engineer, Project Vincent Iowa State University Computation Center + Ames, IA 50011 + 515/294-9551

✗ DCCA-4 Advance Program

Teresa Lunt <lunt@csl.sri.com> Thu, 30 Sep 93 15:09:01 -0700

Advance Program and Registration Information
DCCA-4: Fourth IFIP Working Conference
on Dependable Computing for Critical Applications
January 4-6, 1994
Catamaran Resort Hotel, San Diego, California, USA

Organized by the IFIP Working Group 10.4 on Dependable Computing and Fault-tolerance, in cooperation with:

IFIP Technical Comittee 11 on Security and Protection in Information Processing Systems

IEEE Computer Society Technical Committee on Fault-tolerant Computing EWICS Technical Committee 11 on Systems Reliability, Safety and Security University of California at San Diego

This is the fourth Working Conference on this topic, following the successful conferences held in August 1989 at Santa Barbara (USA), in February 1991 at Tucson (USA), and in September 1992 in Mondello (Italy). As evidenced by papers that were presented and discussed at those meetings, critical applications of computing systems are concerned with 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, 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 methods 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 or fault-tolerance and security, through studies of either a theoretical or an applied nature.

As a Working Conference, the program is designed to promote the exchange of ideas by extensive discussions. All paper sessions end with a 30 minute discussion period on the topics covered by the session. In addition, three panel sessions have been organized. The first, entitled "Formal Methods for Safety in Critical Systems" will explore the role of formal methods in specifying and assessing system safety. The second, entitled "Qualitative versus Quantitative Assessment of Security?" debates of the role that methods based on mathematical logic and stochastic process theory ought to play in assessing system security. The third panel "Common Techniques for Fault-tolerance and Security" explores techniques that are useful for attaining both fault-tolerance and security.

ADVANCE PROGRAM

Monday, January 3

7-10pm Welcome Reception

Tuesday, January 4

9:00-9:15am Opening Remarks

F. Cristian, General Chair

G. Le Lann, T. Lunt, Program Co-chairs

9:15-10:45am Session 1: Formal Methods for Critical Systems Chair: M. Melliar-Smith (U of California, Santa Barbara, US)

W. Tursky, Warsaw University, Poland: On Doubly Guarded MultiprocessorControl System Design

G. Bruns, S. Anderson, U of Edinburgh, UK: Using Data Consistency Assumptions to Show System Safety

10:45-11:00am Break

11:00-12:30am Panel Session 1: Formal Methods for Safety in Critical Systems

Moderator: Ricky Butler (NASA Langley, US)

Panelists: S. Miller (Rockwell Collins, US), M. J. Morley (British Rail/Cambridge, UK), S. Natarajan (SRI International, Menlo Park, US)

12:30-1:30pm Lunch

1:30-3:00pm Session 2: Combining The Fault-tolerance, Security and Real-time Aspects of Computing

Chair: C. Landwehr (NRL, Washington DC, US)

P. Boucher et al, SRI International: Tradeoffs Between Timeliness and Covert Channel Bandwith in multilevel-Secure, Distributed

Real-Time Systems

K. Echtle, M. Leu: Fault-Detecting Network Membership Protocols for Unknown Topologies

3:30-4:00pm Break

4:00-6:00pm Session 3: Secure Systems

Chair: P. G. Neumann (SRI International, Menlo Park, US)

J. Millen, MITRE: Denial of Service: A Perspective

R. Kailar, V. Gligor, S. Stubblebine: U of Maryland: Reasoning About Message Integrity

R. Kailar, V. Gligor, U of Marland, L. Gong, SRI: On the Security Effectiveness of Cryptographic Protocols

Wednesday, January 5

9:00-10:30am Session 4: Assessment of Dependability Chair: W. Howden (U of California, San Diego)

C. Garrett, S. Guarro, G. Apostolakis, UCLA: Assessing the Dependability of Embedded Software Using the Dynamic Flowgraph Methodology

A. Aboulenga, TRW and D. Ball, MITRE: On Managing Fault-tolerance Design Risks

10:30-11:00am Break

11:00-12:30 Panel Session 2: Qualitative versus Quantitative Assessment of Security

Moderator: T. Lunt (SRI International, Menlo Park, US)

Panelists: M. Dacier (LAAS, Toulouse, France), B. Littlewood (City U, London, UK), J. McLean (NRL, US), C. Meadows (NRL, US), J. Millen (MITRE, US)

12:30-1:30pm Lunch

1:30-3:00pm Session 5: Basic Problems in Distributed Fault-tolerant Systems

Chair: F. B. Schneider (Cornell U, Ithaca, US)

C. Walker, M. Hugue, N. Suri, Allied Signal Aerospace: Continual On-Line Diagnosis of Hybrid Faults

A. Azadmanesh, R. Kieckhafer, U of Nebraska: The General Convergence Problem: A Unification of Synchronous and Asynchronous Systems

3:30-4:00pm Break

4:00-6:00pm Session 6: Specification and Verification of Distributed

Chair: R. Schlichting (U Arizona, Tucson, US)

- O. Babaoglu, U of Bologna, Italy, M. Raynal, IRISA, France: Specification and Verification of Behavioral Patterns in Distributed Computations
- P. Zhou, J. Hooman, Eindhoven Univ, The Netherlands: Formal Specification and Compositional Verification of an Atomic Broadcast Protocol
- H. Schepers, J. Coenen, Eindhoven Univ, The Netherlands: Trace-Based Compositional Refinement of Fault-Tolerant Distributed Systems

6:30-10pm: Banquet, with a talk by Peter Neumann

Thursday, January 6

9:00-10:30am Session 7: Design Techniques for Robustness Chair: J. Meyer (U. Michigan, Ann Arbor, US)

- N. Kanawati, G. Kanawati, J. Abraham, U of Texas: A Modular Robust Binary Tree
- R. Rowell, BNR, V. Nair, SMU, Texas: Secondary Storage Error Correction Utilizing the Inherent Redundancy of Stored Data

10:30-11:00am Break

11:00-12:30 Panel Session 3: Common Techniques in Fault-Tolerance and Security

Moderator: C. Levitt (U of California, Davis, US)

Panelists: Y. Deswarte (LAAS, Toulouse, France), B. Littlewood(City U, London, UK), C. Meadows (NRL, US), B. Randell (U of Newcastle upon Tyne, UK), K. Wilen (U of California, Davis, US)

12:30-1:30pm Lunch

1:30-3:00pm Session 8: Real-Time Systems Chair: L. Sha (SEI, Pittsburgh, US)

- M. Goemans, I. Saias, N. Lynch, MIT: A Lower Bound for Faulty Systems without Repair
- S. Ramos-Thuel, J. Strosnider, CMU: Scheduling Fault Recovery Operations for Time-Critical Applications

3:30-4:00pm Break

4:00-6:00pm Session 9: Evaluation of Dependability Aspects Chair: K. Trivedi (Duke U, Durham, US)

G. Miremedi, J. Torin, Chalmers Univ, Sweden: Effects of Physical

some Software Implemented Error Detection Techniques

- J. Dugan, Univ of Virginia, M Lyu, Bellcore: System-Level Reliability and Sensitivity Analysis for Three Fault-Tolerant System Architectures
- J. Carrasco, U Polit de Caalynya, Barcelona, Spain: Improving Availability Bounds Using the Failure Distance Concept

REGISTRATION INFORMATION

Registration fees are \$445 before December 4, 1993 and \$495 afterwards. We will accept a check if it is drawn on a US bank. You may also wire money to the DCCA bank account: Wescorp Federal Credit Union, ABA 122-04-12-19, credit account of USE Credit Union: 32-22-81-691S-025, account UCSD 4TH DCCA, 142665100.

If you register by mail, please make the check out to DCCA-4 and mail with the following registration form to:

DCCA-4

University of California, San Diego
Department of Computer Science and Engineering
9500 Gilman Drive m/s 0114
La Jolla, CA 92093-0114 USA

If you wire money, then please follow up with a letter to the above address, or an e-mail message to dcca@cs.ucsd.edu, or a fax to +1-619-534-7029, or a telephone call to Keith Marzullo, +1-619-534-3729.

REGISTRATION FORM
Name:
Affiliation:
Address:
Telephone number:
E-mail address:
Dietary restrictions:
Registration fees are \$445 before number additional reception December 4, 1993 and \$495 afterwards. tickets (\$35 each): Included in these fees are all lunches, the banquet, and the reception for one number additional banquet person, and proceedings. You may tickets (\$65 each): purchase additional tickets at the following prices: number additional lunch tickets (\$60 each):

HOTEL INFORMATION

The conference will be held at the Catamaran Resort Hotel on Mission Bay (3999 Mission Blvd., San Diego, CA 92109). Please call the hotel to make your room reservations. A block of rooms has been reserved until December 4, 1993 at a rate of \$90 for one or two persons, and \$15 for each additional person above 2. The phone numbers are +1 619 488-1081, fax +1 619 490-3328.

There are flights from most major US cities to the San Diego airport. Transportation from the airport is provided by a company called Super Shuttle, which can be reached by using up the courtesy phone at the Reservation Board near the baggage claim area to call the Catamaran Resort Hotel. The fare is \$6 per person, one way. You can also take a taxi, which should cost \$10-\$15 one way.

All conference events except the banquet will be at the Catamaran Resort Hotel, and lunches will be served at the hotel. The banquet will be aboard the authentically recreated 1800's sternwheller Willaims D. Evans which docks near the hotel. Conference participants may receive telephone calls at the hotel: +1 619 488-1081, +1 619 488-0901 fax.

The hotel is right on the beach on Mission Bay. Winters in San Diego are mild, with daytime temperatures in the low 70's (22-24C) and nighttime temperatures around 50 (10C). Winter is the season in which San Diego gets most of what little rain it gets, so bring an umbrella just in case there is a shower.

CONFERENCE ORGANIZATION

General Chair

F. Cristian, U of California, San Diego, USA

Program Co-chairs

G. Le Lann, INRIA, France

T. Lunt, SRI International, USA

Local Arrangements/Publicity Chair

K. Marzullo, U of California, San Diego, USA

Program Committee

- J. Abraham, U of Texas at Austin, USA
- A. Avizienis, U of California, Los Angeles, USA
- D. Bjoerner, UNUIIST, Macau
- R. Butler, NASA Langely, USA
- A. Costes, LAAS-CNRS, Toulouse, France
- M-C. Gaudel, LRI, France
- V. Gligor, U of Maryland, USA
- L. Gong, SRI International, USA
- H. Ihara, Hitachi, Japan
- J. Jacob, Oxford U, UK
- S. Jajodia, George Mason U, USA
- J. Lala, CS Draper Lab, USA
- C. Landwehr, NRL, USA
- K. Levitt, U of California, Davis, USA

- C. Meadows, NRL, USA,
- J. McLean, NRL, USA
- M. Melliar-Smith, U of California, Santa Barbara, USA
- J. Meyer, U of Michigan, Ann Arbor, USA
- J. Millen, MITRE, USA
- D. Parnas, McMaster U, Canada
- B. Randell, U of Newcastle upon Tyne, UK
- G. Rubino, IRISA, France
- R. Schlichting, U of Arizona, Tucson, USA
- J. Stankovic, U of Massachusetts, Amherst, USA
- P. Thevenod, LAAS-CNRS, Toulouse, France
- Y. Tohma, Tokyo Inst. of Technology, Japan

Ex-officio

J-C. Laprie, LAAS-CNRS, France

IFIP WG 10.4 Chair



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 6

Tuesday 5 October 1993

Contents

RISKs of trusting e-mail

Theodore M.P. Lee

Stocks and Wands

Paul Dorey

Dead for 3 years, but computer kept paying bills

Alan Frisbie

Newton Tale of Woe

Steven Sargent via Paul M. Wexelblat

RISKS of unverified driving records

Mich Kabay

Redundant data

Mich Kabay

Conditioning and human interfaces

Robert Dorsett

Portable phones and fire detectors

Trevor Kirby

Re: Cancer Treatment Blunder

Paul Smee

Re: Security holes and risks of software ...

Bob Bosen

Bank of America fires employee after reading his e-mail?

David Jones

E-mail for denial of services and corruption

Fredrick B. Cohen

Software Quality vs Staff Size

Mike Willey

Info on RISKS (comp.risks)

RISKs of trusting e-mail

Theodore M.P. Lee <tmplee@tis.com> Fri, 1 Oct 1993 11:43:00 -0600

Until such time as either the general population learns what to expect or

digital authentication (such as PEM) becomes widespread, I suspect we will hear more of this kind of incident. This academic year the University of Wisconsin started providing e-mail accounts to all students at its Madison campus. (6,000?, maybe) The students, both technical and non-technical, are being encouraged to use e-mail as a way of interacting with their instructors. They access the accounts either through University-supplied machines scattered throughout the campus or through dial-up Serial Link Protocol (SLIP) connections. A mix of Macintosh's, PC's and other assorted workstations are involved.

Last week (note how early in the school year) a group of five students, several from the Honors floor of one of the freshman dorms, were caught having forged several pieces of e-mail. Most potentially damaging was a note saying it was from the Director of Housing, to the Chancellor of the University, David Ward; note that the previous Chancellor is now Pres. Clinton's Secretary of HHS, so the present Chancellor is new to the job. The forged message was a submission of resignation. Ward's secretary had just returned from vacation and apparently assumed the proferred resignation was legitimate. The secretary accepted it and started to act upon it -- it was only during the course of that that it was discovered to be a fake.

The students also sent messages purporting to be from the Chancellor to other students asking them to pay their tuition. They also forged a message from the Chancellor (my information doesn't say who it went to) saying he was going to "come out of the closet" and announce it Sept. 25.

The students were only caught through a combination of circumstances. First, since they used one of the dial-in connections there were logs of who dialed in when. Secondly, during the course of their experiments they botched some addresses which caused enough traffic to go to the dead-letter office that the investigation could narrow what was happening. (It should be pointed out that the forgery was fairly easy to accomplish using the Eudora mail client on a Macintosh: the user has complete choice over the "from:" field of a message.)

The FBI is investigating whether any federal crime was involved and, needless-to-say, the students are likely to be expelled at the least.

Ted Lee, Trusted Information Systems, Inc., PO Box 1718, Minnetonka, MN 55345 612-934-5424 tmplee@tis.com

Stocks and Wands

<Paul.Dorey@barclays.co.uk>
Thu, 23 Sep 1993 12:30:26 +0100

The market report in the London Evening Standard of 17th September 1993 reported:

...With so many people away from their desks for Yom Kippur there was little inspiration but dealers were startled to see the price of P&O race up from 653p to 863p, triggering thoughts of a dawn raid. The price then disappeared from screens and it was put down to a computer error. The real

price was 603p, up 2p.

[Someone was playing the P&O blindfolded. Perhaps what was needed was a Yom Kippured Herring Aide who could hear "2p on Travel". PGN]

Dead for 3 years, but computer kept paying bills

"Alan Frisbie" <frisbie@flying-disk.com> Sun, 19 Sep 93 17:44:18 PDT

>From the Reuters News Service, printed in The Los Angeles Times Sunday, September 19, 1993:

Computers Paid Bills as Woman in Sweden Lay Dead for 3 Years

Stockholm -- The body of an elderly woman who died in 1990 lay undiscovered in her apartment for more than three years while computers received her pension and automatically paid her bills, Swedish police said Saturday. "It's very unusual for someone to be dead so long without anyone else reacting," a police duty officer in the Stockholm suburb of Farsta told the national news agency TT.

The woman's last-opened mail was dated May 11, 1990, police said, indicating she had died at the age of 72. Her name has not been made public. Police were called to break into the apartment by its landlord after he had made repeated efforts to gain the occupant's permission to renovate it.

Alan E. Frisbie, Flying Disk Systems, Inc., 4759 Round Top Drive, Los Angeles, CA 90065 (213) 256-2575 (voice) (213) 258-3585 (FAX) Frisbie@Flying-Disk.Com

[Also noted by Trevor Jenkins tfj@apusapus.demon.co.uk . The RISKS archives also show a previous similar case. PGN]

Newton Tale of Woe

"Paul M. Wexelblat" <wex@cs.uml.edu> Fri, 1 Oct 1993 13:26:54 -0400 (EDT)

The following was culled from Gene Spafford's Yucks Digest;

I have no idea whather the tale is apocryphal or not, but the implications of putting yet another layer of technology between the mind and the bits (with no sanity clause)...

[Yes Virginia there is a Sanity Clause (cf Groucho)]

anyhow, excerpt follows:

Date: Thu, 23 Sep 93 18:51:39 PDT

From: uunet!frame.com!sbs (Steven Sargent)

Subject: "I think my face is on fire."

To: various

One of my spies on the net reports:

>

> ... I thought you might like to know what Abraham Lincoln would've > said if he'd been writing his notes on a Newton instead of paper.

>

- > "Bookstore avis screen deans ago, our fort fathers brownies
- > front it on fits continent a new nation, concerned in in berry
- and bridge area to fire proposition that air me fire created
- > erasers...."

RISKS of unverified driving records

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 11 Sep 93 15:10:52 EDT

In the Globe and Mail newspaper from Canada for Saturday, Sept 11, 1993, Mary Gooderham, Applied Science Reporter, has an article on page A3 entitled, "Technology points finger at poor drivers: Car rentals could become more difficult as motorists' records are shared."

The article explains that for \$5, the Ontario Transportation Ministry will provide any registered driver's record (including name, license number, date of birth, sex, conviction--criminal and highway--and accident history. Such information is supposedly restricted to "authorized requesters" including police, collection agencies and insurance companies.

In contrast, the province of British Columbia will being in October 93 to require written permission from data subjects before releasing their accident records.

Gooderham writes that some US rent-a-car agencies routinely check the driving record of applicants from NY, MD, FL and OH. Poor drivers are refused service.

In Canada, the Interprovincial Record Exchange is managed by the Canadian Council of Motor Transport Administrators, which is considering "giving third parties access." In NY, TML Information Services serves as broker between the State and rental-car agencies. According to Gooderham, TML's CEO, Sean Doherty, expects "half of U.S. drivers will be covered by the system by the middle of next year."

+ + +

The prospect of reducing road accidents and thefts by keeping track of rotten drivers and no-goodniks appeals to my orderly side. However, in the light of extensive discussions in RISKS-14 about faulty credit, driving, and criminal records, the lack of clear information or procedures for _checking_ and

correcting such records is a problem. How would you, a model citizen and driver, like to discover on the morning of your vacation/business/emergency trip that you appear to have been disqualified by an erroneous database record? Arguing with the poor soul on the other side of the counter will clearly not help. I expect to see a growing number of lawsuits as a result of database errors or possibly even program bugs when innocent people suffer from data corruption.

It will not be good enough to allow just _anyone_ to make ostensible corrections in our records, either. Some method of identification and authentication will have to be devised to prevent nasty people from damaging other people's histories.

And just what, pray, will that entail? A national identification card? Perhaps we are headed that way. The social security number is already becoming an equivalent that can tie together many independent databases to provide a detailed vision of an individual's personal and professional life.

Without adequate provisions for maintaining data integrity and validity, the growing use of databanks containing personal information will result in costly and perhaps dangerous errors.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Redundant data

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 11 Sep 93 15:11:34 EDT

As a followup to the article on drivers' records I just posted, I would like to explore the consequences of having many interlinked but independently-managed databanks describing us. These problems have been familiar to data processing personnel for the last 50 years, but they will be new to some of the designers, administrators and users of interlinked personal-information databases being established throughout government and industry.

Agency A maintains a databank and links in to Organization B, which links up with Institution C. Data flow from A -> B -> C. An error creeps into the record for Percy Perfect in database A. It propagates to B and C.

Percy discovers the problem one morning when he lands at Seattle Airport and tries to pick up his Superior Rent-A-Car vehicle so he can make a 10 am meeting 120 miles away in the back woods of Washington state. He is refused because his record now shows that he stole a car in Florida 3 years ago. Actually, Percy has never stolen as much a jellybean in his life and has never been to Florida. It's one of those identity-mixups. Oops, sorry, we'll fix it.

Three weeks later, the correction finally makes it into database A.

Question: is there a mechanism in place to record the fact that the record had in the past been sent to database B? And will B also "know" that it ought to

send a correction to database C?

If all works well, there is no problem.

But what if C doesn't "know" that B got data from A. What if A, not "knowing" that C got some of _its_ data from B, signs an agreement to begin sharing data FROM C? Then we have A -> B-> C -> A: a circular data path.

As soon as there is a loop in the topology, the loop may inadvertently become an accumulator or buffer. So A send a correction to B which propagates it to C, but unfortunately just moments before the correction arrives, C ships an update to A showing the erroneous data. Will A update its own new records with an old record that is in fact wrong? Yes it will, unless provisions are implemented to forestall such problems.

Some of the techniques that will have to be evaluated include

- o time stamps using coordinated time to allow a system to establish which of two records is newer.
- o a standardized format for exchanging the _history_ of a record: where did it come from? when?
- o mechanisms for unique identification of a database.
- o mechanisms for alerting member databases to circular references.
- provision for authentication of updates; perhaps message authentication codes in the style of ANSI X9.9, including a sequence number in the MAC to prevent insertion and deletion of transactions.

A printout of the data subject's record should be delivered to the data subject on demand when and where the information is used. In addition, as a means of catching errors fast, it would help if a printout were delivered to the data subject every time the record is modified. These practises would not prevent or identify all problems (e.g., they'd fail when the address is wrong) but at least they'd be on the right path.

The Internet contains files which co-exist in different repositories without too much conflict. Let us hope that this model of collaborative data storage will serve as an example of how to accommodate redundant data without bureaucratic and governmental meddling.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Conditioning and human interfaces

Robert Dorsett <rdd@cactus.org> Fri, 1 Oct 93 05:32:34 CDT

After testing a computer-based training program last night, on a PC, it was time to quit. The program used a GUI-ish interface, one of those home-

grown interfaces that appeared on the PC before Windows became established.

So, I selected quit, saw the prompt, and hit "no." Automatically. Then returned to the main menu. Did this three times, very fast, figuring I missed the button. Finally, my host said, "Try clicking on yes."

The prompt? "Do you want to quit?" Yes/No.

But *I*, a Mac-user, have been conditioned to see: "Save changes before quitting?" Yes/No/Cancel. This is the only time you see "are you sure" prompts on exiting a Mac program. I was just screwing around, so of COURSE I hit "No."

I'm sure there's a RISK in there, somewhere...:-) It was COMPLETELY instinctive for me to hit "No"...

And while I'm at it, an old vending-machine story, which someone suggested I send to RISKS at the time. This was one of those machines with an alpha A-F "category" selector, with a numeric item selector. So if you wanted the fifth item on row C, it would be C-5. After entering the proper amount, one hit the button "C", then the button "5."

Except in this case, the item was C-11. What did I, techno-nerd, do? "C-1-1." Twice. Getting the item C-1. Then I looked down, and saw that the numeric selectors went down to 12, including 10, 11, and 12. Oh.

In this vein, airliner avionics requiring numerical entry tend to use "phone-style" keyboards, with 123 the top row of keys. Yet all calculators are exactly the opposite, with 123 the second-to-bottom row. What happens when cultures clash, in THAT case? :-) Or the 0 key is transposed from the left bottom-most key, to the right? Or put to the left of the 1? :-)

Profound questions at 5AM....

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

portable phones and fire detectors

"Trevor Kirby" <Trevor.Kirby@newcastle.ac.uk> Fri, 1 Oct 93 13:01:53 BST

Michel E. Kabay was wondering about the risks of new digital phones on microprocessors. I don't know about this but I do know that using certain types of portable phone near certain types of fire detectors can set off a false alarm.

The problem was caused by portable phones causing an ionization detector to send out a signal which was interpreted by the system as a genuine detect. The problem came to light when the customer used a portable phone to complain

about the late arrival of the engineer, needless to say he was sat right under one of the detectors.

Trev

Re: Cancer Treatment Blunder (Randell, RISKS-15.05)

Paul Smee <P.Smee@bristol.ac.uk> Fri, 1 Oct 1993 10:28:19 +0000 (GMT)

Brian.Randell@newcastle.ac.uk wrote:

- > Details of the errors were disclosed after a clinical inquiry by senior
- > radiologists who examined the cases of all 1045 patients who had
- > radiation doses of up to 35% less than prescribed. Their report blamed
- > human error by Margaret Grieveson, a physicist, who unnecessarily
- > programmed a correction factor into the radiography computer in 1982."

The inquiry has indeed blamed Dr Grieveson, but from the news reports it is not totally clear to me that this is fair - there are some unanswered questions.

The nature of the error is that she manually instructed the new computer controlling the X-ray to apply a standard correction factor (as had been required previously) based upon the distance of the radiation source from the patient. Unknown to her, however, the computer program already had this correction coded into it, so that in essence it was being applied twice.

It's the 'unknown to her' that bothers me, and that the reports have not addressed. Does this imply that she didn't bother to RTFM, or is it the case that the manufacturers of the equipment thought it so obvious that the program would include the correction, that they didn't bother to mention it? I'd really like to know.

Whichever is the case, it clearly demonstrates the risk of changing methodologies without making absolutely certain that everyone fully understands the new methods, and how they compare to the old ones.

Finally, if the board of inquiry is able to determine, merely by reference to the set of records which were routinely kept, that patients were consistently being underdosed, then it feels probable that a review of the case papers in each individual case, while treatment was going on, could have revealed the same thing. Does this also demonstrate the risks involved in changing procedures without creating a mechanism for monitoring the effects of the change?

★ Re: Security holes and risks of software ... (Peterson, RISKS-15.05)

Bob Bosen

+ Bob Bosen

- Bob Bosen <b

- > The interesting part is that for the first time we are approaching the point
- > where true separation is possible. Not in a mainframe, nor in a UNIX machine
- > but in the client-server network (not peer-peer though).
- > IMHO this changed world-view is going to cause the single greatest change in
- > information security that we have ever seen. Networks will cease being
- > "unsecurable" and become the only accepted means for protection of data.

I hope you're right, Padgett, but we've got a LONG way to go. It's amazing how many network users are unaware of the ease with which packets can be monitored, copied, and replayed. Every time I present my lecture on public-domain software tools to monitor LAN segments, most of the audience is shell-shocked!

-Bob Bosen- Enigma Logic Inc.

✓ Bank of America fires employee after reading his e-mail?

David Jones <djones@cim.mcgill.ca> 1 Oct 1993 12:55:50 -0400

I read a fax of a photocopy of a newspaper article (sigh), which unfortunately had the name of the newspaper as well as the date and author of the article are obscured. Although I am confident this is authentic, please keep this source in mind.

"This is the new field of what [...] calls
'electronic voyeurism'. [...]
The results of electronic peeping are as
troubling as they are bizarre.
Supervisors with no intent to do mischief
may watch employee message traffic on computer systems.
That kind of surveillance led a major California
financial institution, the Bank of America,
to fire an employee after his electronic mail
indicated that, when his day job ended,
he worked nights as a professional gay stripper."

- (1) Can anyone out there supply more factual details about this case? It must have hit the papers in California.
- (2) We are left with a legal morass ...
 - (a) At least in Canada, public and private institutions do have the right to monitor "private communications", but only if their intent is to check the performance and security of the systems that they are responsibile for maintaining. By the way, one might argue that the date, time, volume, originator, recipient of communications should be sufficient for this purpose, making perusal of the contents, under the guise of checking performance or security, questionable.

[caveat: the absence of a "reasonable expectation of privacy" makes listening much easier, as in cellular phones, or product support phone calls to an employee in the service dept of a company -- these issues are orthogonal to the following...]

- (b) Privacy laws protect personal communication.
- (c) Some Universities have rules of the following nature:
- (i) it is against policy to read another person's files or e-mail.
- (ii) a person's personal files and e-mail *are* admissible as evidence against an accused person.

One might imagine that (ii) is ineffective because while it says personal files and e-mail can be used, (i) says no one can ever obtain them! Implicit in the presence of (ii), however, is the notion that if such personal information *magically* appears at the pubic printer and is handed to someone evaluating the accused, then ... so be it.

A motivated technical person could even conveniently "suspect" a problem with the computer or communications system, totally eviscerating the privacy rule, by appealing to (a).

E-mail for denial of services and corruption

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Thu, 30 Sep 93 03:48:34 PDT

I just did an experiment sending massive quantities of e-mail to a typical Unix box, and of course, I was able to overrun the disk capacity on the recipient machine, thus making the system grind to a crunching halt for lack of space. Since I sent it to daemon, nobody noticed the mail for quite some time, and it took a bit before they figured out the problem and were able to fix it.

I don't know for sure, but I think a lot of systems are susceptible to this attack, and there is no easy solution, at least if you still want to get mail.

To assess the degree to which this might be a threat, I got a listing of DoD and US Government sites from the Chaos Computer Club (thank you Charles) and tried sending mail to them - only 1 refused the mail out of 67 tried. Several told me there was no such mail recipient, but gave me a directory of other recipients with simnilar names - how helpful. A few told me they didn't have such a user and identified that they were a particular type of system - now I know for certain what UID to send to.

Under some versions of Unix, you can put quotas on users, but not on e-mail space - as far as I know. The ULIMIT prevents unbounded growth, but it is now set high enough by default on most systems that it won't stop this

attack. You can explicitly refuse mail on some systems, but I don't think there is a general way to do this selectively enough to defend against this attack. The default is almost always to get all that comes to you. Your suggestions are welcomed - FC

Software Quality vs Staff Size

Mike Willey <mwilley@feenix.metronet.com> Wed, 22 Sep 1993 08:34:36 -0500

My company is involved with a client that is producing a device that will be used in open heart surgery. Our responsibility is the design and implementation of the electronics and software that will control this device.

Our client is pushing to increase the staff size 2 to 3 times beyond the number of individuals actually required to do the work. Our contention is that "too many cooks spoil the broth", an oversized staff is less likely to produce a high quality, safe product.

Does anyone in these news groups have information on acedemic or industry references relating to this subject, pro or con? FDA or military project histories would be especially useful.

Thanks for the help. Mike Willey



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 7

Weds 6 October 1993

Contents

ISDN telephone glitch in Hamburg

Klaus Brunnstein

Japan: IT Security, JCSEC criteria Klaus Brunnstein

Re: The FBI investigating college pranks Fredrick B. Cohen

Re: Conditioning and human interfaces

Robert Dorsett

Re: Answers to the mail problem Fredrick B. Cohen

Trusted portions

Fredrick B. Cohen

Think of it as an opportunity, not a problem A. Padgett Peterson

Re: Risks of Unverified Driving Records

Robert J Woodhead

Jim Cook

Rex Black

CFP "Ethics" Workshop Cuba Feb.1994

Klaus Brunnstein

Info on RISKS (comp.risks)

ISDN telephone glitch in Hamburg

Klaus Brunnstein

brunnstein@rz.informatik.uni-hamburg.d400.de> Fri, 17 Sep 1993 14:07:38 +0200

On September 16, 1993, about 12,000 Hamburg based customers of Germany's new ISDN digital telephone system were hit by a software bug from which telephone services could be recovered only after almost 12 hours. Mainly commercial users (about 25% of Hamburg's presently 50,000 ISDN customers) were unable to use their telephone, fax and data services until after noon.

According to a German Telecom official, the problem arose when a new software

was loaded on the ISDN control systems, at 2:00 am. Probably due to a bug, systems crashed and subsequently also refused to load the old software. Only at 1:15 pm, system engineers succeeded to restart the old system version.

ISDN is the Integrated Services Digital Network, which allows to transmit all sorts of communication (fax, telex, texts, data, telephone calls) via a digitized network with one type of connector box. At this time, out of 1,2 Mio telephone customers, 50,000 have yet ISDN based system, including the author's faculty, with daily bad experiences about broken calls, false connections, devices beeping for no rationale reason etc. Fortunately, the author's telephone set was operating in the "usual" way during this blackout.

Klaus Brunnstein (Uni-Hamburg, September 17, 1993)

[By the way, someone PLEASE tell Klaus that his mail addresses --- both d400 and dbp --- no longer work from my system! Something broke. PGN]

Japan: IT Security, JCSEC criteria

Klaus Brunnstein klaus Brunnstein & klaus Brunn

It is not well recognized in the current discussions in North America and Europe aimed at harmonizing their different criteria (FC, ITSEC) that Japanese organisations are undertaking major efforts to assess and improve the state of IT and Communications security also in their country. In order to guarantee their IT industries' opportunities in international markets, they are also looking for a minimum harmonized set of criteria (JCSEC) as a basis of universally applicable product evaluation and certification.

Among others, Information-technology Promoting Agency (IPA) and Japan Electronic Industry Development Association (JEIDA) have started their respective work with major analyses of the state-of-security in Japan, North America, Europe and Australia. IPA, a MITI funded organisation with interests in AntiVirus measures, sponsored a study which received some attention in 1992. Its basic statement was that the number of hacker-like attacks on systems doubled in recent times while virus infections diminished significantly. It is interesting that IPA's recent statistics about viral events in Japan sharply increased in 1993: from 1990's total 14 events over 1991's total 57 events and 1992's 252 events, the partial figures in 1993 (Jan-July) are 366. While findings in Mac (less than 10 reports) and so far 19 viruses having appeared on the (IBM-incompatible) Japanese PCs (15 reports in 1993) are constant, the very fast growth of IBM compatible PCs is based on 42 different viruses, with 166 Yankee Doodle, 103 Cascade 1701/1704, 24 Anti-Telefonica, 20 Stoned III or Michelangelo and 14 Form reports in 1993. Though IPA's request for reporting virus events is now known in many enterprises, these figures do NOT indicate the exact number of infections but only show the relative development: growth.

As its basis for future work, JEIDA has published a "Summary Report on the Worldwide Survey for Information Systems Security in Nine Nations", conducted by Coopers & Lybrand, in March 1993. The survey which is based on 1,059

questionnaires filled from enterprises in Japan (39%), Australia (21%), North America (15%) and Europe (13%) analyses the state of security consciousness (chapter 1), experience with incidents (ch.2: e.g. malfunction of hardware>75%, introduction of viruses >30%, theft of equipment about 10%, disclosure of Passwords: 10%, etc), and IS Security Measures taken (a rather detailed analysis, ch. 3). An analysis of the Cost of IS Security Measures (ch. 4) and IS Risk Analysis (ch. 5), Motivating Factors (ch. 6) and Development Priorities (ch. 7) concludes this study (17 pages). For detailed analysis, it would be helpful to complement the hi-quality color print with a volume containing more details of the raw data, but this "JEIDA Study" is worthwhile to read for worldwide comparison.

JEIDA published another study in August 1992 "Japanese Computer Security Evaluation Criteria: Functional Requirements (Draft V1.0)" which has not been recognised so far in the Western discussion (similar to Russia's development, published in December 1992, though in Russian). JEIDA's study (in English), developed after MITI guidelines, describes (ch.1: Introduction) Functionality Requirements, with scope of the "Target of Evaluation" (TOE) and Target Models, and gives detailed "Functional Requirements" (ch.2), including minimum requirements for Identification and Authentication (2.1), Access Control (2.2), Accountability (2.3), Auditing (2.4), Object Reuse (2.5), Integrity (2.6), Reliability of Service (2.7) and Data Exchange (2.8). Though the structure conforms with ITSEC concerning the 8 basic function categories, JCSEC evidently follows US' Minimal System Function Requirements philosophy which is also basic to ECMA's (European Computer Manufacturers Association) and ISO/IEC JTC1 SC 27 works. The report (26 pages) ends with a graph describing the different security criteria in USA, Europe, Japan and ISO, followed by a glossary with informal definitions of essential terms.

Though the Assurance part of JCSEC has not been published so far (due end-of-1993), it seems as if ITSEC's Assurance levels may play the role of related "Minimum Assurance Requirements" (rather than the complex Assurance descriptions in US' Federal Criteria).

JEIDA officials motivated their work in JCSEC generally with their vendors' experience when having attempted to sell Japanese IT systems in Australia. Following regulations for Australian government installations, which seem also to be applied by major Aussie enterprises, Japanese installations had to undergo a security evaluation process which was partly difficult as most documents were not available in English. When being forced to prepare evaluation and certification of their products in non-Japanese countries, MITI and Japanese vendors evidently concluded that a set of internationally harmonized criteria with minimum requirements would serve their interests best. Moreover, Japanese vendors seem to favour self-evaluation of security functions, as opposed to an evaluation by independent institutions as practiced or prepared in USA and Europe. As some of these ideas are shared also by IT vendors outside Japan (see ECMA's approach), the Japanese involvement may add fresh wind to the international ITSEC discussion which is presently dominated by USA/Canada and Europe (including their preoccupations :-)

Klaus Brunnstein (Univ-Hamburg, September 16, 1993)

PS: JEIDA's address is: Japan Electronic Industry Development Association,

JEIDA, Kikai-Shinko-Bldg., 3-5-8 Shiba-Koen, Minato-ku, Tokyo 105 JAPAN.

★ Re: The FBI investigating college pranks

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Wed, 6 Oct 93 05:00:48 PDT

It's a sad state of affairs when the FBI investigates a college prank but doesn't investigate murder and rape running rampant through the nation. When I was in college, students sent a resignation letter from the Dean of Students to the President on official letterhead. There was no federal investigation, and the most any student would ever get for such a prank would be a stern lecture about being sociable. If they investigated half the pranks the FBI would be forever chasing kids around our college campuses. Lets keep some perspective on things and spend our federal time and money on something more useful. - How about a study of how many times a butterfly flaps its wings before it dies? FC

★ Re: Conditioning and human interfaces (Sosman, RISKS-15.06)

Robert Dorsett <rdd@cactus.org> Wed, 6 Oct 93 19:57:09 CDT

- > ... Mr. Dorsett's point (perhaps) should be that there ought to be a> Standard Standard... But are today's interfaces so good that we're> willing to discourage innovation?
- There's no innovation in these approaches. They are all on the same cognitive level, using similar display and input mechanisms. They are merely different permutations of a theme, often guided by no "philosophy," just GUI extensions of old-fashioned CLI-style prompts.

So, in this case, yes, there is only one credible type of solution, and, yes, especially when PC's are trying desperately to turn into Macintoshes, and when huge segments of society are used to standard keyboard formats, some standard heuristics should apply, one way or the other.

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

Answers to the mail problem

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Wed, 6 Oct 93 10:02:47 PDT

Three answers came up that I thought might be worth sharing:

1 - Some versions of sendmail have a capability to refuse mail after disk space is reduced to a specified constant. This resolves the flooding problem but does not allow legitimate mail to pass.

- 2 Some people think you should have a separate disk partition for mail and News (where this apparently happened regularly to some people by accident), which solves the problem except of course it denies legitimate mail.
- 3 Some systems allow user-based quotas under which mail falls, but in many systems this doesn't work because the superuser delivers the mail, and thus the legitimate user is run out of space while the system is also run out of space. Some people mentioned that they hadn't tried limiting quotas to all system user but that it would be necessary to limit the impact of this problem.

Most respondents said that they felt this was a fairly common state of affairs. In other words, as delivered, systems don't handle this well, and most systems administrators don't know how to, aren't aware of, don't have the time to, or for whatever reason don't do anything about this problem.

I wonder how many things besides mail and news create this possibility. Does anyone know of any other information sent to a system that automatically (by default) consumes disk space? It would be worthwhile to classify these things and keep them in a common place so we know that a particular partition has them all, and know where to look. P.S. I make one partition per disk to get rid of the stupidity of having to keep things in different directory structures just because my computer isn't smart enough to figure it all out. It only hurts under a few circumstances, and it makes life easier in a lot more of them.

We received a large amount of mail on this topic, including that from sater@cs.vu.nl (Hans van Staveren) rogerb@x.co.uk (Roger Binns) mathew@mantis.co.uk (mathew) andyc@cappsdv2.fob.ford.com wfg!mdavis@uunet.uu.net (Michael T Davis) taylort@dg-rtp.dg.com (Tad Taylor) .

Several suggested that THEIR mailers are not so stupid, and suggested various well-known ways of handling the problem. Thanks. PGN]

Trusted portions

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Wed, 6 Oct 93 10:02:47 PDT

Trusted portion should be small, but then there is the problem of the interface between the trusted and untrusted portions of the program. One way to deal with this is via a cryptographic interface between authorized and unauthorized portions of programs. Another alternative is to have the trusted program verify the integrity of the untrusted program. Just a thought. - FC

P.S. I have had a small trusted program for separating trusted from untrusted segments of programs for quite some time, and it works well, but it's not all that easy to use correctly. - FC

Think of it as an opportunity, not a problem (Re: Willey, RISKS-15.06)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Wed, 6 Oct 93 08:25:04 -0400

[Was: Software Quality vs Staff Size]

"The customer is always right". One approach that was inspired by several other RISKS entries would be to split the group into 2 or 3 teams and give each one the same requirements. When each is done feed the same test cases in and see what the results are. Once they always agree, pick the best/fastest/most elegant one & deliver.

Once upon a time, "safety of flight" dictated IV&V (independent verification and validation) of all software. IMHO many of the RISKS postings have indicated that even simple quality control is a thing of the past.

Two years ago my wife was in an automobile accident that required removal of the battery from our car. Yesterday I had occasion to disconnect the battery & discovered that Godzilla must have replaced it, probably with an impact wrench. The terminals were screwed on so tight that the attachment post ripped out of the battery before loosening, causing an acid leak (yes, I was turning it the right way 8*(, and ruining the battery.

Latent software errors are like that, sometimes taking years to show up, and are caused much the same way -- someone operating without supervision and outside their field of expertise. In my experience with programming, (and that goes back longer than I would care to admit) very few "programmers" really understand the systems they are working on -- certainly very few people worldwide understand the BIOS in a PC yet this is what makes a PC "100% compatible".

There are over 150,000,000 PCs worldwide now, probably less than 500 people who have any understanding of the BIOS (and half of them write viruses). Yet what would one expect the architecture for that medical device mentioned in to be ? Would anyone be surprised if there was an Intel iapx 80x86 based system inside ?

Maybe it is time for certification, at least for devices that are safety related.

Padgett

★ Re: Risks of Unverified Driving Records (Kabay, RISKS 15.06)

Robert J Woodhead <trebor@foretune.co.jp> Wed, 6 Oct 93 20:52:57 JST

In <u>RISKS-15.06</u>, Mich Kabay writes about the Risks of unverified driving records, and the problems of an erroneous record leaving one stranded at the airport sans auto.

There is a simple solution that avoids most of the problems; the Car rental companies should be allowed to refuse to accept a reservation, but not cancel one once it has been made. Thus, the client would be asked when he phoned for the reservation for his driver's license number.

This would have the side-effect of giving the driver an early warning that there is a problem with his record (either a real problem with his driving, or someone elses typing problem)

Robert J. Woodhead, Biar Games / AnimEigo, Incs. trebor@forEtune.co.jp AnimEigo US Office Email (for general questions): 72447.37@compuserve.com

★ Re: Risks of Unverified Driving Records (Kabay, RISKS 15.06)

Jim Cook <jcook@epoch.com> Wed, 6 Oct 93 11:20:38 EDT

In commenting on shared driving records, Michel E. Kabay comments:

"It will not be good enough to allow just anyone to make ostensible corrections in our records, either. Some method of identification and authentication will have to be devised to prevent nasty people from damaging other people's histories."

I really have to comment on this:

Suppose you suddenly find yourself with a bad record one day. It only took one person a few minutes to accidentally or deliberately make this erroneous error one day. What level of authorization did that person have? Frequently, very little.

Now you want to correct it. What level of authorization do you need? Frequently, you probably have to go through heck and high water to do so. And consider the time factor: the entry was made in a minute. The correction takes weeks.

Think about credit records. This has all come up before. And there you often are not allowed to expunge the record, rather, just add a correction below (if at all).

I understand Michel's sentiment to prevent wrong-doing. But from everything I read, it's the legitimate that have been losing out.

C. James Cook, Epoch Systems, Inc., 8 Technology Drive, Westboro, MA 01581 508-836-4711x385 JCook@Epoch.com

Re: Risks of Unverified Driving Records (Kabay, RISKS 15.06)

Rex Black <rex@iquery.iqsc.com> Wed, 6 Oct 93 10:09:45 CDT I think Mich's suggestions are excellent. Certainly the subject should have the right to verify information which directly affects his quality of life. However, I don't think this will entirely resolve the problem, because it doesn't cover some crucial economic issues.

Most data collection agencies are for-profit corporations. While they have an interest in selling reasonably accurate data to their clients, their clients value the data most from the point of view of _preventing_ a business decision that results in a major loss. In the car rental example given, the rental agency looks for background data that proves "badness". The risks for both purchasers of the data and the data subjects arise when the purchaser of the data is attempting to use the information to exclude a bad-risk subject. However, note that, while the data purchaser bets a possibly substantial amount of money that the data will identify bad risks, and the subject bets substantial inconvenience and possibly money that the data will not incorrectly finger him/her as a bad risk, the data provider risks virtually nothing in any transaction. I say "virtually" because, if the agency fails to identify bad risks often enough, the data purchaser may choose another data provider. However, the agency may misidentify good risks as a bad ones a number of times without consequence to it, and it is unlikely that the injured party in this circumstance (the subject) will convince the data purchaser to dump the data provider on the basis of his injury.

So, we have a situation wherein the data collection agency risks less by keeping negative data on subjects, even if it is questionable, than it does by eliminating negative data. This fact, combined with the relative financial positions of the data collection agency and the data purchaser versus the data subject, puts the subject (i.e., us) at a significant disadvantage. As far as I can see, the only remedy to this aspect of the problem lies in making the data collection agency itself directly liable for all injuries to the data subject arising from errors in its data. If our hypothetical traveller is denied a car and must take a \$1,000 round-trip cab ride to Bumbaloosa, east Washington to make his business meeting, then WRT Data Services should legally owe him \$1,000 (plus court costs if necessary) for the incident.
Additionally, they should be liable for punitive damages if the same erroneous data causes a similar (or worse) injury at a later data. The first liability gives them an incentive to correct the error, and the second liability gives them an even stronger incentive to prevent the error from recurring.

While I hate to advocate legislation that will increase litigation, the unfortunate fact is that, without laws and lawyers to level the playing field, those of us on whom others keep and sell data will remain permanently at risk from bad data. It is in our interest to push for such legislation now, before the data collection agencies become immovable by the Congress (c.f., the insurance companies).

Rex

✓ CFP "Ethics" Workshop Cuba Feb.1994

Klaus Brunnstein
 strunnstein@rz.informatik.uni-hamburg.d400.de>

Mon, 13 Sep 1993 17:31:54 +0200

CALL FOR CONTRIBUTIONS for an IFIP WG 9.1 Workshop, from Ina Wagner

ETHICS AND SYSTEMS DESIGN: THE POLITICS OF SOCIAL RESPONSIBILITY Havana, Cuba, February 17-19, 1994

IFIP has been for some time analyzing the possibility of developing its own Code of Ethics. Working Group 9.1 Computers and Work is planning to contribute to the discussion on political and ethical problems in systems design, beginning with a small workshop. The main focus of this workshop will be

- * to discuss grounded scenarios which can provide rich knowledge of the political and ethical problems encountered in a variety of contexts,
- * to analyze the relationships between ethics and the politics of work in these contexts (including the work environment of systems designers),
- * to develop practical guidelines that help the professional community of systems designers to identify political and ethical dilemmas and to respond to them.

THEMES OF THE WORKSHOP

Ethics and the Politics of Systems Design:

We think of ethical problems as emerging wherever the values and moral principles on which individuals base their decisions and actions are contested or in conflict. Such conflicts between people's values, norms of conduct and claims for moral ground often point to basic underlying differences between their positions in the organization or in a society, their interests, and, consequently, their assessment of certain situations. In that respect, ethical problems have a strong political content.

Real life situations are often characterized by ethical dilemmas involving the co-existence of conflicting or competing values. The ethical problems that emerge in a field are shaped by its conditions and contexts, as are the conflicts that arise between different ethical principles, their different perception and evaluation by different actors in the field, and the solutions that participants look for and finally come to accept. Although high standards of individual responsibility (as represented in an ethical code) are indispensable, these need organizational support in order to unfold and develop. Consequently, the politics of systems design itself need to be a primary focus of all deliberations on professional ethics. Questions of personal morality stand a chance of becoming significant guidelines for action only if the systemic questions are openly discussed. Among these are the work practices and working conditions of systems designers -- management and development practices as well as the paradigms within which systems designers are working.

Learning from ethical scenarios:

Ethical scenarios should be grounded in the analysis, development and use of information technology in different contexts. We think that rich descriptions of actual conflicts and of how participants cope with them might sharpen systems designers' awareness of ethical problems in general,

support their analytical understanding and help them enter a dialogue with others in the field. As WG9.1 we are particularly interested in exploring the relationships between ethics and the politics of work.

Making ethical principles practicable:

Generalized "ethical codes" have the advantage that they can act as some basis for a minimal social standard to be taken into account in systems design. They oblige systems designers consciously to connect their technical analysis of a problem with a moral-practical judgement. Two requirements for such general ethical principles are:

- * Their formulation should make clear the consequences of an adequate, responsible attitude for the relationships between all participants in a design effort.
- * They should clearly express the difference and tension between the obligation to observe professional norms on one hand and to depart from these norms if other principles or the situation make this necessary".

We look for suggestions on how such codes could be developed and made understood and practicable.

Institutional frameworks for social responsibility:

One particularly difficult task is to set up an institutional framework for implementing an ethical code and to define the legitimate actors in such a framework. Analysis of the composition of ethical committees in the medical area, for example, has brought forward the problems involved in deciding whether some people are more "affected" or more worthy of participation in decision making than others because of their education, social background, specific merits for society or their minority position. Experiments with citizen participation in communal projects often use drawing lots among the general constituency instead of elective procedures.

Another question is whether members of such an institutional framework should be representative of particular groups. It could for example be argued that otherwise underrepresented actors should be over represented. This could be justified in a number of ways: A critical mass of members from that group may be necessary to give weight to their perspective; there should be sufficient room for the particular values and interests of this group to be heard.

We look for contributions that deal with these issues on a theoretical and practical-empirical level (discussing cases, practices).

OUTLINE OF THE WORKSHOP

Participants are invited to submit either:

a) Ethical scenarios from different types of work organization (from hospitals to industrial sites) and different cultures (including developing countries) which are suitable for an in-depth discussion.

An ethical scenario should

* be informed by a real case (or cases),

- * include some temporal/historical/developmental account,
- * describe ethical/political conflict in relation to the working conditions and professional culture of the different communities of practice involved in the case.

or

b) a Position Paper which deals with one (or several) of the leading issues of the workshop.

Short versions (2-4 pages) should be submitted to:

Ina Wagner, Vienna Technical University, Center for CSCW
Argentinierstrasse 8, A-1040 Vienna, Austria
Tel: +43 1 58801 4439 Fax: +43 1 5042478 Email: iwagner@email.tuwien.ac.at

They will be reviewed by the members of the Programme Committee.

OUTCOMES OF THE WORKSHOP

One main result of this workshop will be a position paper for the Reader on Ethics and Computing edited by Jacques Berleur, Chair of the IFIP Ethics Task Group. An additional possibility is to revise and expand some of the contributions for publication in an international refereed journal.

KEY DATES

November 1, 1993 Deadline for submission of short version

December 1, 1993 Notification of Acceptance

Given the short preparation time, authors are not expected to send in full papers before the conference. However, once accepted they will be given instructions on how to prepare their contribution for the conference itself.

PRACTICAL INFORMATION

This conference will be connected to the WG9.4 Conference "The Impact of Informatics on Society: Key Issue for Developing Countries" (from February 21-23 also in Havana). If you are interested in participating in this event as well, please contact:

Prof. Sam Lanfranco
Centre for Research on Latin America and the Caribbean (CERLAC)
York University (Room 240YL)
4700 Keele Street, North York
Ontario, Canada, M3J 1P3
phone: (416) 736-5237

fax: (416) 736-5737

email: lanfran@vm1.yorku.ca

Information on the conference site and accommodation will follow. Cuban Airlines as well as Iberia offer moderately priced flight & accommodation arrangements. We will inform you about the possibilities in time.

WORKSHOP FEE

As we have no funding for this conference, we would appreciate participants to contribute a registration fee (beyond expenses).

Full registration fee: US\$ 200 Reduced registration fee: US\$ 100

PROGRAMME COMMITTEE

Andrew Clement (University of Toronto), Vice Chair WG9.1 Mike Robinson (University of Aarhus) Lucy Suchman (Xerox Park, Palo Alto) Ina Wagner (Vienna Technical University), Chair WG9.1



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 8

Thursday 7 October 1993

Contents

Control faults cause train crash

Hank Cohen

- WSJ report on potential problems with 757/767 Autopilots **PGN**
- Typing error causes stock to fall 20% for `a few moments' Lorenzo Strigini
- Epitope suit uses computer bulletin board

Tom Hanrahan

Libraries

Phil Agre

The Panoptic Sort

Phil Agre

"Change" and October 1993 CACM

Jim Huggins

Mailing list fun

Mark Brader

Virus distributed during college computer sale

Jim Huggins

Re: Bank of America fires employee ...

Robert Ellis Smith

Re: RISKs of trusting e-mail

Bob Frankston

Re: The FBI investigating college pranks

Valdis Kletnieks

Separating parts in privileged applications

Yves Royer

A reference on Ethics

Peter B Ladkin

Re: Cancer Treatment Blunder

David Crooke

Jerry Bakin

PGN

Info on RISKS (comp.risks)

Control faults cause train crash

<hank@westford.ccur.com>
Thu, 07 Oct 93 03:29:42 EDT

Excerpted from The Japan Times October 7,1993

Osaka- Osaka Prefectural Police suspect control faults caused a train to crash here Tuesday, injuring 178 of the 290 passengers on board. They suspect the driverless train was traveling at about 30 kph when it crashed into a safety buffer at Suminoekoen Station, judging by the number of broken glass panels on the train.

The train derailed after smashing into the buffer at the end of the track. Had it passed through the buffer, it would have crashed down on to a major street which was filled with rush-hour traffic. [The train was elevated approximately 20 meters judging from TV pictures. It would have had to crash through both the buffer and a short concrete wall at the end of the track before it could have fallen to the street. HKC] Of the 178 injured passengers, 48 were hospitalized.

It was the first time the New Tram has been involved in an accident causing injury since it began running in 1981 The train, which carries about 60,000 passengers each day, makes about two-thirds of its runs without a driver or conductor aboard.

Similar computerized transport systems are being introduced in Kobe, Saitama and Yokohama. [A similar train is already in operation near Nagoya. HKC]

Malfunctions of the train's two control systems led to the crash, police said. The automatic train operation system, which decelerates the train in four stages when it is within 200 meters of a station, failed, and the automatic train control system, which stops the train in an emergency situation worked inadequately, they said.

The control system applied an emergency brake only 45 meters from the safety buffer by using an emergency circuit, police said.

Hank Cohen, Concurrent Nippon Corp., Shuwa yanagibashi Bldg. 5F, Yanagibashi 2-19-6, Taito-ku Tokyo 111, Japan Denwa: 03-3864-5714 Fax: 03-3864-0898

✓ WSJ report on potential problems with 757/767 Autopilots

Peter G. Neumann < neumann@csl.sri.com> Thu, 7 Oct 93 11:26:59 PDT

WALL STREET JOURNAL (October 7, 1993) - Federal safety investigators said autopilot problems have caused certain Boeing jets to change direction for no apparent reason. The National Transportation Safety Board has asked the Federal Aviation Administration to warn pilots that autopilots on Boeing 757 and 767 airplanes have engaged and disengaged on their own, and to take precautionary measures. The FAA said it would put the matter under "high-priority review." The autopilots of Boeing 757s and 767s are made by Collins Avionics, a division of Rockwell International. Collins officials couldn't be reached to comment.

Milano: Typing error causes stock to fall 20% for `a few moments'

Lorenzo Strigini <strigini@iei.pi.cnr.it> Thu, 7 Oct 93 13:28:35 MET

Excerpted and paraphrased from "la Repubblica" (popular, "independent" Italian morning newspaper), 28 September 1993, p. 54 (quotes, square-bracketed comments and mis-translations of stock market jargon are mine):

"The day in Piazza Affari [i.e., the Milano Stock Exchange] was characterised by a curious incident": an operator was ordered to sell 51000 'Generali' shares at 39,500 Lire each; he mistyped the price as 35,000. "The mistake prevented Generali stock from 'opening' and caused turmoil in the market: what calamity was happening in Italy or the world so severe ... to make the price of the best stock in the Italian market drop so quickly? A few moments of panic followed, which caused a further drop of the price to 31,000 Lire. Then the mystery was explained, and Generali closed at 39,991 Lire (+1.18 %) and at the end of the day they were exchanged above 40,000 Lire."

As I understand it, the stock market is protected against snowball effects from such mistakes by the fact that authorities can stop the dealing on an item whose price changes too quickly; I wonder whether any of the software used by individual dealers attempts to alert them about seemingly extravagant orders.

Lorenzo Strigini, IEI-CNR, Via Santa Maria 46 I-56126 Pisa - Italy tel. +39 50 593495; fax +39 50 554342 E-mail: strigini@iei.pi.cnr.it

Epitope suit uses computer bulletin board

Tom Hanrahan <hanrahan@sequent.com> Thu, 7 Oct 93 08:40:21 -0700

From The Oregonian (Portland, Oregon), October 7, 1993, by Vince Kohler

Epitope Inc. used information subpoenaed from the computer bulletin-board service Prodigy to prepare a \$5 million federal lawsuit against a Kidder, Peabody vice president in Kansas City, Mo.

Lois Rosenbaum, a lawyer for Epitope, said the company used information from Prodigy Services Co. to track down A. Karl Kipke, who works for Kidder, Peabody in Kansas City, Mo. The lawsuit claims that Kipke used a false name, William Smith, to log onto a Prodigy electronic bulletin board on three occasions in August. Each time, the lawsuit contends, Kipke wrote lengthy commentaries he knew were false and defamatory about Epitope, the company's management practices and its attempts to gain federal approval of an oral device used to detect the AIDS virus.

[...] "We certainly believe the price of the stock is lower than it would've been but for these false allegations, Rosenbaum said. "And I think it's clear that the articles were written for the purpose of negatively influencing the price of the stock." [...] Epitope's lawsuit says Kipke and his clients were holders of short positions in Epitope stock. [...] Epitope's lawsuit seeks \$5 million in punitive damages from Kipke and alleges defamation, manipulation of

security prices, securities fraud and intentional interference with business

Rosenbaum acknowledged that the lawsuit's electronic dimension is "a very unusual situation."

Submitter note: The omitted sections of text basically say that Kipke was unavailable for comment and explain what holding a "short position" means.

-- Tom Hanrahan, hanrahan@sequent.com

Libraries

Phil Agre <pagre@weber.ucsd.edu> Wed, 6 Oct 1993 17:50:59 -0700

The Spring 1993 issue of the journal Representations (orange cover, widely available on newsstands in college towns) is a special issue on the future of libraries, taking as its point of departure the new national library that Francois Mitterand is trying to build in Paris. The whole issue is interesting, but the main Risks-relevant article is by Geoff Nunberg:

Geoffrey Nunberg, The place of books in the age of electronic reproduction, Representations 42, 1993, pages 13-37.

Nunberg argues (among many other points) that printed newspapers have served to help create what Benedict Anderson called "imagined communities". The idea is that, since everyone in San Diego (say) gets more or less the same version of the San Diego Union-Tribune, readers of the Union-Tribune are aware that everyone else who is reading the paper sees the same articles. Thus they can get a sense of what "everyone knows" about the day's events that help to knit together a coherent concept of the community. Of course in San Diego people read the LA Times and the NY Times as well, and many people get all their news from TV. The point is that people get their news from only a small number of sources that are the same everywhere, and these provide a way of imagining what "we" know, think, read, have opinions about, and so forth.

In the age of electronic distribution of information, though, it's quite possible for everyone to get customized information which is filtered down in various ways and then assembled from a patchwork of different sources. The result might be greater difficulty in imagining communities, as opposed to imagining professions or other specialized interest groups that would tend to steer toward the same information sources.

The same issue contains an article on the future of copyright:

Jane C. Ginsburg, Copyright without walls?: Speculations on literary property in the library of the future, Representations 42, 1993, pages 53-73.

Phil Agre, UCSD

The Panoptic Sort

Phil Agre <pagre@weber.ucsd.edu> Wed, 6 Oct 1993 16:52:46 -0700

The current Harvard Business Review contains an article telling business people how to use massive databases of personal information in their marketing. Although generally somewhat weak, it does include some special moments, like the observation that most businesses can't yet afford enough disks to store tens of millions of bytes (including, for example, purchase histories) on tens of millions of customers. The most useful bit is a sidebar on pages 154-155 explaining that privacy restrictions on uses of personal information only hurt small businesses, since the big ones can afford the added costs they induce. This lame argument is a good example of the current big fashion in lobbying, "showing how it hurts the little guy". The reference is:

Jim Bessen, Riding the information wave, Harvard Business Review 71(5), September-October 1993, pages 150-160.

The same issue includes an equally vague article on enterprise integration.

The good news is that a really interesting new book on personal information has appeared:

Oscar H. Gandy, Jr., The Panoptic Sort: A Political Economy of Personal Information, Boulder: Westview Press, 1993.

It's helpful to consider the book at three separate levels:

- (1) It includes an impressive catalog of phenomena related to personal information. Most of these will be familiar from Risks, but here they're all collected in one place with references. It also includes a remarkable survey of the relevant critical literature, for a total of about 700 useful footnotes.
- (2) It also includes some empirical studies, some of which I found more useful than others. The best by far is a study of the conditions under which people become concerned about threats to privacy from the collection of personal information. It has all the limitations of survey and focus group based research, but it's an important starting point.
- (3) Finally, it attempts to develop a theory of the political economy of personal information. It is a pessimistic theory, laying out the forces that tend to cause personal information to be collected and centralized. As such, this theory will not please conservatives, with their faith in markets, or progressive activists, with their faith in people's capacity to resist oppression. But hey, maybe he's right.

Phil Agre, UCSD

✓ "Change" and October 1993 CACM

Jim Huggins <huggins@eecs.umich.edu> Thu, 7 Oct 1993 14:08:22 -0400 (EDT)

How ironic.

In the October 1993 issue of CACM, the "Inside RISKS" column contains a long litany of computer systems which were proposed as new and better alternatives to existing systems, but rarely were completed "on time, within budget, and up to spec."

In the same issue, the "Newstrack" column reports on the recent announcement of plans to build an IBM supercomputer with 512 processors at Cornell. New York Governor Mario Cuomo comments, "I really don't understand it, but I know it means change; and from change comes strength."

Perhaps -- but as "Inside RISKS" demonstrates this month, change which is not carefully planned and carefully executed may bring weakness, too. The attitude that "if I do it on a computer, it's better, and if it's on a bigger computer, it's better yet" still seems far too prominent.

<msb@sq.com>
Thu, 7 Oct 1993 19:39:58 -0400

The "Rich Bastard" bank mailing list blooper (<u>RISKS-14.89</u>) was also posted to alt.folklore.computes, where it spawned a thread on incorrect transformations of personal and other names in mailing lists.

The following are collected from articles by John Miller, John Switzer, Jeff Hibbard, Jay Maynard, Joel Sumner, Jeff DelPapa, Hugh JE Davies, Terry Kennedy, Jake Richter, Kevin Stevens, Scott Telford, and Brad Heintz. Remarks in ["..."] are from the above people and not me.

Georgia-Pacific Corporation

- -> Georgia P. Corporati
- -> Dear Ms. Corporati ["So how long have you been an Italian transvestite and how did the bank find out about it?"]

Bradley University

- -> Mrs. Bradley Un, IV
- -> Dear Mrs. Un

James R. Maynard III

-> Mr. Iii [but in the same software...]

James R. Maynard, III [but "I've always signed my name without the comma"]

-> Mr. Maynard

Lambda Chi Alpha

-> Alpha, Lambda C.

Undergraduate Lounge

- -> Dear Mr. Ung Lounge,
- -> Just think what the neighbors will think when they see you and the other members of the Lounge family riding around the neighborhood in your new Cadillac. ...

Lord xxxx

-> Dear Mr. Lord

St. Peter's College

- -> Saint Peter S. College
- -> Dear Saint College ["It's amazing that they actually parse for a salutation of 'Saint'. How many of those are still receiving mail?"]

Citibank

-> Pending Deletion, Citibank

Department of Computer Science

-> Dear Mr. Science,

Nuclear Physics Department

-> Dear Mr. Nuclear [The recipient "put it on his door, thus buying himself an instant nickname."]

And finally

["I had been sharing a house rental for several months, a few years back, when we received a dunning notice from a collection agency. ... Took a bit of the pace off that it was personalized to 'Resident', though."]

Mark Brader, Toronto utzoo!sq!msb msb@sq.com

[PGN adds that the RISKS archives include bunch of others that could be included in this list, the most amusing of which were probably these:

Friedman Wedd etal

-> Etalfried Wedd [a letter offered the recipient a pre-approved loan for \$750. A follow-up spoof story given in RISKS-10.16 had "Etalfried" complaining about the paltriness of the amount, and being offered an unsecured cash loan for \$250,000!]

Mail sent to Switzerland

-> wound up routed to Switzerla ND (North Dakota).]

Virus distributed during college computer sale

Jim Huggins <huggins@eecs.umich.edu> Thu, 7 Oct 1993 13:48:08 -0400 (EDT) The University of Michigan annually holds a "Computer Kickoff Sale", an opportunity for students to buy personal computer systems through UM for reduced prices. This year, a few students got an added bonus: a virus.

Four hundred Macintosh systems sold on the first day of the sale had the nVIR virus included on the standard distribution disks prepared by the Information Technology Division (ITD). The source of the virus is currently unknown.

"We're still investigating where the virus may have come from ... We don't know if it's the duplicating company that we used, it's a possibility. It's a possibility that even though our master disks here were scanned for viruses before it went out to the duplicator, it could have been infected here," said Phil Harding, manager of the sales program.

The standard distribution disks include a copy of Disinfectant, a Macintosh anti-viral program, which can be used to remove the nVIR virus. ITD warned new users about the possibility of viral infection even before this problem came to light. ITD has removed the virus from all remaining distribution disks and will replace any old distribution disks free of charge.

Ryan Goble, a first year student who bought a Macintosh through the sale, commented, "I assumed everything would be sterile because the disk came in a plastic bag."

Harding again: "Next year we'll have tighter controls and testing. I'm assuming responsibility for this because it was under my jurisdiction. We just have to do tighter testing once the disks come back from the duplicator." Later: "It's a bad situation, but we're trying to make the best of it. I'm sure this incident will make people more aware of viruses and to get the right applications to eradicate and prevent them from occurring."

[Source: cover story in _The_Michigan_Daily_, UM campus student newspaper, 7 Oct 1993.]

★ Re: Bank of America fires employee ... (Jones, RISKS-15.06)

Robert Ellis Smith <0005101719@mcimail.com> Thu, 7 Oct 93 02:24 GMT

David Jones in Montreal asked about a report that Bank of America fired an employee after snooping in his e-mail and discovering that he worked as a male stripper at night. It is true that Bank of America fired the man, Michael Thomasson of San Francisco after it discovered his moonlighting, but they discovered it by going through his desk, not his e-mail. This case and 500 other invasions of privacy are written up in WAR STORIES, a collection published by Privacy Journal and selling fo r \$17.50. Call 401/274-7861 or write MCI Mail, rsmith 510-1719, or PO Box 28577 Providence RI 02908.

While we are at it, Privacy Journal also publishes a special report on uses and abuses of Social Security numbers, including the current laws covering the use of SSNs. It sells for \$15.

Robert Ellis Smith Publisher, Privacy Journal

✓ Re: RISKs of trusting e-mail

<Bob_Frankston@frankston.com> Wed, 6 Oct 1993 23:35 -0400

Forgeries of resignations and the like are the norm during the novelty phase of a service. Of course many people will treat it as a very serious crime.

My concern is more with the issue of closed loop vs open loop mechanisms. There will always be some imperfections in the system that people will exploit on purpose or by accident. While we can string offenders up by the thumbs, accidents will still happen. For example, one needs to send a quick message and uses the nearest terminal forgetting that it will be from the currently logged in user.

People need to remember that reality checking is a key part of any system be it technical or social. If one receives an unexpected letter of resignation, one should check it out instead of playing the role of a droid and just following through. There will still be the serious crimes in which one sets the stage so the letter seems real, but casual pranks should have bounded repercussions. Of course, if people verified, we'd lose too many book and movie plots.

In a world where legal communication is via Fax the problem is not just "computer" fraud but one of assuring a degree of trust.

I do recall a store where some students at MIT submitted an order for a 747 from Boeing. They got a call asking where to deliver it...

The report on the error in radiation dosage also emphasis the open-loop phenomena. Why doesn't a life critical system meter the actual dosage given instead of assuming that everything is working perfectly. Then there was the BART Train that couldn't determine it was going at 40mph when it thought it was stopped.

★ Re: The FBI investigating college pranks (Cohen, RISKS-15.07)

Valdis Kletnieks <valdis@black-ice.cc.vt.edu> 7 Oct 1993 21:10:33 GMT

>It's a sad state of affairs when the FBI investigates a college prank but >doesn't investigate murder and rape running rampant through the nation.

On the other hand, the FBI is only chartered to investigate certain categories of crimes. In particular, they can only initiate action on violations of *federal* laws, or assist in state or local actions *on invitation only*. Now, if a "college prank" involves the violation of one of the federal statutes regarding electronic activity, they can take action. Murder and rape are state actions and handled at the state level (hint - read the papers about

ongoing trials, and see if they are being held in the state court system, or in the local Federal Circuit courts).

The legal basis for this setup goes back to the Constitution and the delegation of powers to the federal and state governments.

Does anybody have a reference to which federal statutes the FBI used as a basis for the investigation?

ObRisk: Do we, as a nation, *want* the FBI sticking its nose into every murder and robbery case? I'm sure there's a Big Brother problem lurking there..

Valdis Kletnieks, Computer Systems Engineer, Virginia Tech

Separating parts in privileged applications

<Yves_Royer@uqtr.uquebec.ca>
Thu, 7 Oct 1993 15:43:13 -0400

When an application runs with more than one privilege state, care should be taken to isolate the privileged portion from the untrusted code. This is well done with ring protection schemes:

Address space is organized in "rings", from the inner kernel (lowest ring number, highest privilege) to the unprivileged application (highest ring number, lowest privilege).

A program can only CALL routines of same or HIGHER level of privilege. A routine of lower privilege is considered untrustable: You call the operating system, don't expect it to call you. Hardware enforces that the routines are called only at special entry points called "GATES".

When a routine executes in a more privileged state, it's address space and stack is isolated from access by less privileged routines by being placed in another ring space. A program can ACCESS data of same or LOWER privilege. Of course, a privileged program should not really trust what lies (pun intended ;-)) in less privileged spaces.

Some routines can conform to the ring of the caller. For example a well debugged string manipulation routine is very trustable and can be used by the operating system as well as the application, but should not be granted increased privilege when running.

Code has three ring attributes:

- a) Least privileged ring where it can execute. The code is not accessible from programs which lack this access level.
- b) Least privilege granted. If this value differs from the first one, the routine is said to be "GATED", and can execute with a higher privilege than the caller. If the caller uses the routine at a privilege level equal or higher, then the execution ring do not change.

c) Most privileged ring where it can execute (ie: Trust level)

The routine is untrustworthy of usage by a more privileged application.

In ring numbers, the relation $a \ge b \ge c$ is always true.

Data has two ring attributes:

- Read attribute: Least privilege needed to read the information.
- Write attribute: Least privilege needed to write it.

The write ring level is always lower or equal than the read level (same or higher privilege)

Files possess ring attributes. In such a system, the password file could be world readable and writable, but in rings which normal users cannot normally access.

The separation of address spaces ease the debugging of system problems: When data integrity is compromised in an address space, the lower-privileged routines and programs are not likely causes for the problem, unless the address spaces manager is itself in error in some way.

Of course, there are drawbacks. The over-utilisation of ring mechanisms augment context switches (which are costly), and the processor needs more registers to manage the rings. The only operating system I know that uses this protection scheme fully is NOS/VE.[*] I know that the 80x86 (x > 1) have a built-in ring mechanism and that OS/2 uses it to some point, but I do not know of any UNIX system that uses rings.

A network implementation using this scheme could be interesting, but hardware address space separation should be replaced by cryptographic certificates. A client-server implementation would be slow compared to the hardware solution, but it would be more portable.

Yves Royer, Universite du Quebec a Trois-Rivieres (819) 376-5100 Yves Royer@UQTR.UQuebec.CA

[Never heard of Multics, eh? Well, that was almost 30 years ago. ... PGN]

A reference on Ethics

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 6 Oct 93 18:44:45 BST (Wed)

Readers concerned with ethical issues in computing might be interested in the article: Is There an Ethics of Computing? by Geoffrey Brown in the J. of Applied Philosophy 8(1), 1991.

Peter Ladkin

★ Re: Cancer Treatment Blunder (Smee, RISKS-15.06)

<dcc@dcs.ed.ac.uk> Wed, 6 Oct 93 15:20:23 BST

Paul Smee asked if the radiation machine operator forgot to RTFM -- apparently the hospital didn't receive the manual until several YEARS after they started using the machine!

David Crooke, Department of Computer Science, University of Edinburgh JCMB Rm 3310, King's Bldgs, W Mains Rd., Edinburgh EH9 3JZ. 031 650 6013

Re: Cancer Treatment Blunder

Jerry Bakin <JERRY@INNOSOFT.COM> Tue, 05 Oct 1993 22:36:11 -0800 (PST)

What kind of testing did they do?

I would hope that testing this device would include a test to make sure it was calibrated. That if the machine is supposed to operate at so many roentgens for so many seconds, that it actually does so!

This would not be a built-in-test, but would involve an external, precalibrated measuring instrument.

Let's get real, when I buy bananas and gas, those scales are required to be inspected in such a manner!

I would have hoped that this test would have been performed:

By the manufacturer:

- o after every relevant hardware or software change
- o on each machine before it is shipped

At the clinic:

- o upon delivery and acceptance of the machine by the radiologists
- o whenever maintenance is performed
- o at periodic intervals (annually, quarterly?)

Who built this, the same dolts who tested the Hubble mirror?

Dare I suggest some official body regulate such devices, or would that be an example of government over regulation of private industry?

Jerry Bakin.

★ Re: Cancer Treatment Blunder

RISKS Forum <risks@csl.sri.com> Wed, 6 Oct 93 8:41:07 PDT Yes, but regulation is not enough. You must have seen the item in RISKS about the gas station that had Trojan horsed its computer and was systematically charging for gas that had never been pumped. PGN

★ Re: Cancer Treatment Blunder

Jerry Bakin <JERRY@INNOSOFT.COM> Wed, 06 Oct 1993 11:07:56 -0800 (PST)

You're right. But regulation would raise the issue, and create paper trails to show some compliance. There's not much motive to charge for radiation that hasn't been pumped, although I guess that IS exactly what had been occurring. My hope is that was unintentional in the cancer treatment case. :)

Jerry.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 9

Friday 8 October 1993

Contents

Risks of disrupting air traffic control ("Mile High Club")

Richard Marshall via Tom Blinn

Sound of the Fury, Part II

Peter Wayner

Risks of "security" on Apple Newton

Doug Siebert

Re: Control faults cause train crash

Dik T. Winter

Marc Horowitz

Re: Conditioning and human interfaces

Nick Rothwell

Re: Separating parts in privileged applications

Paul Karger

Steen Hansen

A. Padgett Peterson

Re: "Change" and October 1993 CACM

Selden E. Ball

<u>Jr.</u>

James K. Huggins

Re: Libraries and Imagined Communities

Mark Gonzales

Re: Cancer Treatment Blunder

Bob Frankston

Rogier Wolff

Jon Jacky

Re: RISKS of unverified driving records

Jim Horning

Jim Hudson

Info on RISKS (comp.risks)

✓ Risks of disrupting air traffic control ("Mile High Club")

"Dr. Tom Blinn (DTN 381-0646, ZKO3 3X05)" <tpb@zk3.dec.com> Fri, 08 Oct 93 14:39:08 +28716

I'm sure there are multiple risks here -- not the least of which is that the reported incident disrupted ATC communications for about 50 minutes. [Dr. Thomas P. Blinn, UNIX Software Group, Digital Equipment Corporation Mailstop ZKO3-3/W20, 110 Spit Brook Road, Nashua, New Hampshire 03062]

----- Forwarded Message

Subject: :-) BRITISH COUPLE BROADCAST THEIR FROLIC IN THE SKIES

From: MOVIES::RMARSHALL "Richard Marshall 824-3383 EDO-13 08-Oct-1993 1611"

Subj: This looks true as air traffic in and out was disrupted that night...

(Our Technical Director was returning to Edinburgh from London that night and was delayed...)

RTw 10/06 2320 BRITISH COUPLE BROADCAST THEIR FROLIC IN THE SKIES

LONDON, Oct 7 (Reuter) - A British couple who made love in a light aircraft forgot to turn off their transmitter and broadcast their moments of passion to air traffic controllers and radio enthusiasts on Wednesday.

The couple, flying in a private Cessna 150 plane near the Scottish city of Edinburgh, began by debating whether they should have sex 5,000 feet (1,500 metres) above ground and join the "Mile High Club." Their conversation grew more and more passionate and then ceased.

"We've been trying to raise you for the past 50 minutes," an angry controller was quoted by the domestic Press Association (PA) as telling the errant couple when they came in to land. "We've been listening to your conversation. Very interesting. Please come and see me when you land."

Fifteen aircraft, including shuttles, holiday jets and cargo planes, had to use an emergency channel while the two cavorted.

PA said the pilot reported to the authorities at Edinburgh Airport, where he was carpeted for blocking radio communication. "Apart from one aspect of his airmanship -- his failure to check in on a regular basis -- there were no breaches of aviation rules," PA quoted the airport's air traffic control manager Paul Louden as saying.

[No breeches, either. Gives a new meaning to "Beam me up, Scotty!" PGN]

Sound of the Fury, Part II

Peter Wayner <pcw@access.digex.net> Mon, 4 Oct 1993 15:15:35 -0400

Several months ago, I noted that AT&T was planning on using its submarine finding acoustical expertise to track the ebb and flow of traffic on the highways. This Sunday's NYT (Oct 5, pg 30) mentioned that another company, Alliant Techsystems of Edina, Minn is trying to get the Federal Government to buy a system from them and install it in Washington, DC. The target?

Targetshooters.

They aim to place a network of sensors on top of telephone and utility poles and link them into an array that would allow the police to track random gunfire and respond much faster. (Up to 85% faster according to the article.) There would be no need to wait for a good citizen to call and report the reports.

The author (Warren Leary) spent some of the ink wondering whether such a project was actually feasible. Several accoustical experts were "skeptical about whether sensors could be designed to isolate gunshots from other city noise." But the RISK is not just that the project will turn into a fool's folly. Some of the city noises that might not be filtered out are conversations...

Risks of "security" on Apple Newton

Doug Siebert <dsiebert@icaen.uiowa.edu> Wed, 6 Oct 1993 19:47:26 GMT

The Apple Newton has a "security" feature which involves letting the owner/ user set a password to the machine, presumably to protect private data stored in the machine. Its possible of course to get it to dump its data to a Macintosh for backup purposes, where it can be easily sifted through. But readers of this group probably would expect that. Maybe even some users would expect it. But something I was surprised to find out is that in that data dump the user's *plaintext* password is stored! Given the number of people who use the same password for about everything requiring a password, it is easy to see what the risks are here...

Doug Siebert dsiebert@isca.uiowa.edu

Re: Control faults cause train crash (Cohen, RISKS-15.08)

Dik T. Winter < Dik.Winter@cwi.nl> Fri, 8 Oct 1993 02:26:45 GMT

It appears computer controlled trains are not yet there. Although my experience did not have casualties it points to some problems. The London Docklands Light Railways are completely computer controlled. There is a conductor/driver on board for emergencies, and the closing of doors. Moreover, he has to take control on the station (Canary Wharf) the software is not yet able to deal with after all those years of operation.

What we experience was that at the terminal station the train stopped as intended, but a few centimeters short of the exact required place. The net result was that the doors refused to open. The conductor/driver had to come forward to the driving box to manually forward those few centimeters. But this happened only after a prolonged conversation with the Central Control.

So apparently (but this is just speculation) there are sensors that tell

whether the doors can be opened and there are different sensors that tell whether a train is where it should be. And they do not always agree.

--

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland home: bovenover 215, 1025 jn amsterdam, nederland; e-mail: dik@cwi.nl

★ Re: Control faults cause train crash (Cohen, RISKS-15.08)

Marc Horowitz <marc@MIT.EDU> Thu, 07 Oct 93 23:29:13 EDT

<> 60,000 passengers each day ...

Lets see. That's 262.8 million passengers. 178 injuries and 48 hospitalizations means that 1 in 1.5 million passengers is injured, and 1 in 5.5 million is hospitalized. This isn't the 1 in 10^9 figure we hear often on this list, but it's a fairly admirable record, nonetheless.

Failing controls are certainly a RISK, but one must look at the entire record, not just a single bad incident.

Marc

★ Re: Conditioning and human interfaces (Dorsett, RISKS-15.06)

Nick Rothwell <cassiel@cassiel.demon.co.uk> Fri, 8 Oct 1993 10:41:35 +0100

>I'm sure there's a RISK in there, somewhere...:-) It was COMPLETELY >instinctive for me to hit "No"...

There's a quite obvious risk. At one time I was using versions of EMACS on UNIX and on the Mac. The command set common to both is identical, except for the behaviour upon quitting if there is unsaved work, which looks roughly as follows:

(GNU Emacs) Save changes to buffer FOO before exiting? (Y/N) (microEmacs) One or more unsaved buffers exist, quit anyway? (Y/N)

After I'd been caught by that a couple of times, microEmacs hit my bit bucket with a resounding clang.

Nick Rothwell | cassiel@cassiel.demon.co.uk

CASSIEL Contemporary Music/Dance | cassiel@cix.compulink.co.uk

Rings (was: Separating parts in privileged applications)

<pkarger@gte.com>
Fri, 08 Oct 93 10:00:48 -0400

Monsieur Royer mentions NOS/VE as using protection rings, and Peter Neumann points out that Multics is of course the classic example of the first operating system to use rings. However, many other systems since then have also used rings including:

VME/B for the ICL 2900 AOS/VS for the Data General MV8000 VMS for the DEC VAX the Hitachi 5020 time sharing system (first with hardware rings)

and probably many others.

- Paul

Separating parts in privileged applications (Royer, RISKS-15.08)

Steen Hansen <steen@kiwi.swhs.ohio-state.edu> Fri, 8 Oct 93 08:05:48 -0400

> [Never heard of Multics, eh? Well, that was almost 30 years ago. ... PGN]

The Primos operating system uses this ring protection scheme. It was developed by a number of the same people who made Multics.

Steen Hansen e-mail: hansen+@osu.edu

Computer Specialist (614) 292-7211 (Stores/Food: tue/thu/fri)
Ohio State University (614) 292-9317 (Dentistry: mon/wed)

Separating Parts in Privileged Applications (Royer, RISKS-15.08)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Fri, 8 Oct 93 08:50:08 -0400

While such a ring mechanism *can* be quite effective. It must be remembered that all such schemes (including the "protected" mode of the 80286+) rely at some point on software to effect the state change. While this can be effective protection at the OS level, it is vulnerable in every instance I have seen to a tunnelling or covert channel attack.

Conventional cpus (and the Intel iapx architecture in particular) are single state machines and a properly presented instruction will be executed by the hardware. If only software deciders are used to determine whether to change rings and the higher rings are also implemented in software, they can be bypassed.

Years ago in a galaxy far, far, away I had a problem with an OS that operated in such a "protected" state and would periodically update its real time clock with an "unmaskable" interrupt. We needed a precise 660 usec period without any interrupts to the executing code. By placing an array at the head of the program and storing a value into a reverse dimension - clk(-2078)

as I recall - it was possible to turn off the clock while our code executed.

Padgett

★ Re: "Change" and October 1993 CACM

Huggins, <u>RISKS-15.08</u> <"Selden E. Ball, Jr." <SEB@LNS62.LNS.CORNELL.EDU<> Fri, 8 Oct 1993 10:29 EDT

In addition to the RISKS posed by the computing systems themselves, there are risks when one tries to analyze computing systems from limited information.

In RISKS-15.08, Jim Huggins <huggins@eecs.umich.edu> made some comments about a system being implemented in Cornell's Theory Center. Unfortunately, as best I can tell, his comments were based solely on a single paragraph in _Communications of the ACM_, October, 1993, v36, n10, p11: "NEWSTRACK -- POWER HUNGRY".

As a result, Jim seemed to be trying to apply standards which are usually appropriate when evaluating production computing facilities. Although it has been an extremely useful tool for many of the people using it, the highly parallel IBM computer system that was mentioned is still a (rather expensive) research project. By definition, research always entails "risk".

More information about the research facilities at Cornell's Theory Center, one of the NSF funded national supercomputer centers, is available from their gopher server at gopher.tc.cornell.edu, port 70.

Selden E. Ball, Jr., Cornell University, Laboratory of Nuclear Studies 230A Wilson Synchrotron Lab, Ithaca, NY, USA 14853-8001 +1-607-255-0688

★ Re: "Change" and October 1993 CACM

"James K. Huggins" <huggins@eecs.umich.edu> Fri, 8 Oct 93 10:39:44 EDT

Selden is right, of course: the new research project at Cornell is far different than the large projects chronicled in "Inside RISKS", and I don't mean to disparage this particular research project. My point may have been obscured by my attempt to be a little too cute.

My critique is more of Cuomo's voiced attitude that "change brings strength". I wonder how many of the large projects whose failures are discussed here got started because some government official or corporate bigwig said "If we do this with a computer, it will be better," without thinking through *why* it would be better if done with a computer. Such an attitude needs to be challenged (though more carefully than I did).

★ Re: Libraries and Imagined Communities (Agre, RISKS-15.08)

Mark Gonzales <markg@ichips.intel.com> Fri, 8 Oct 1993 17:12:51 GMT

>...aware that everyone else who is reading the paper sees the same articles.

Unfortunately computer based publishing of paper newspapers has already broken the "imagined community". In Portland Oregon where I live, the local newspaper, the Oregonian, publishes separate sections of local news for downtown, and each of the suburbs. Subscribers living in suburb A only get the local news for their suburb, remaining ignorant of goings on in suburbs B,C,D and E. So two randomly choosen readers are likely not to have received the same articles.

This is already having effects on local politics. There was a letter to the editor this week from a political activist[*] on a State-wide issue complaining that the efforts of his co-campaigners in suburb A are only reported in suburb A's local news section, thus voters in the other suburbs are deprived of news on how the campaign is being fought.

Mark Gonzales

[*] he is one of the opponents of the Oregon Citizens Alliance second State-wide anti-gay rights campaign.

Re: Cancer Treatment Blunder

<Bob_Frankston@frankston.com> Fri, 8 Oct 1993 10:59 -0400

At the Risk of being overly brief:

Regulation isn't an answer. I presume there is already regulation against building devices that kill more patients than necessary. How does one inspect new technologies? I've been told, for example, that there are regulations on digital X-rays that prevent storing high resolution images. This is based on some notions of standardization.

RTFM isn't the answer. The quality of documentation is inversely proportional to cost of a device and negatively correlated with the need for a manual. A printed manual is a great example of an open-loop device. It just sits there in its own reality. For customizable equipment the odds of it all coming together with the corresponding versions of everything are very low. Of course, by the same reasoning, you shouldn't comment your code since comments and execution paths don't necessarily cross nor stay in synch.

Re: Cancer Treatment Blunder (Randell, RISKS-15.05)

Rogier Wolff <wolff@liberator.et.tudelft.nl> Fri, 8 Oct 93 16:31:01 +0100 I think the REAL risk in this case would be that the doctors at the "defective" machine would write a paper saying that they get much better results when they use higher doses than customary. That would lead to OVERDOSES being applied at different sites to different patients.

Roger

★ Re: Cancer Treatment Blunder (Bakin, RISKS-15.08)

Jon Jacky <jon@violin1.radonc.washington.edu> Fri, 8 Oct 93 12:56:08 -0700

I work in a radiation therapy clinic, so I had to respond to this recent RISKS posting:

- > I would hope that testing this device would include a test to make
- > sure it was calibrated. That if the machine is supposed to operate at
- > so many roentgens for so many seconds, that it actually does so!

Well, of course they're calibrated! Every modern therapy machine has two independent dose monitoring channels (both independent of the control the operator uses to select the dose) that measure the dose emerging from the machine. At most clinics these are calibrated *every morning* against a completely independent reference which is not part of the machine at all.

In fact, all of these procedures were probably being followed at the clinic in question, as I understand the incidents described in this thread. As I heard it, the blunders involved a different issue entirely, which postings here have seemed unaware of.

The hard part of the problem is determining what machine output will deliver the prescribed radiation dose *at the tumor in the patient's body*, accounting for absorption of some of the beam in the overlaying tissue, irregular patient geometry, etc. This involves a whole additional set of measurements and calculations, some of which must be done differently for each patient, and which are largely independent of the machine control system itself. My understanding is that the errors involved this part of the process.

> Who built this, the same dolts who tested the Hubble mirror? ...

This remark illustrates a tendency that we sometimes in RISKS and elsewhere. Someone learns of a mishap through a very brief and incomplete news account, makes a lot of assumptions about what must have happened, proposes an obvious remedy, and is smugly sure that *they* would not have been so careless. But in fact the news reports are incomplete, the reader's understanding is oversimplified and naive, and the proposed safeguards (and some the reader didn't think of) are already in place --- but didn't work in this particular situation. We have reached a stage where our technological systems are very complex, most of the obvious things have already been seen

to, and there really aren't so many "dolts" out there in positions of responsibility.

- > Dare I suggest some official body regulate such devices, or would that
- > be an example of government over regulation of private industry?

There is already some regulation of people, clinics and devices. I'm sure some of it helps, but just as there is a limit to what you can allow to go unregulated, there is also a limit to the degree of oversight it is reasonable to expect from regulators. To put this all in perspective, radiation therapy mishaps are very rare, especially in view of the large number of patients treated, and the potential hazards.

Jonathan Jacky, Radiation Oncology RC-08, University of Washington Seattle, Washington 98195 (206)-548-4117 jon@radonc.washington.edu

Re: RISKS of unverified driving records

<horning@src.dec.com>
Thu, 07 Oct 93 12:44:22 -0700

This is a typical instance of problems caused when one organization supplies (possibly erroneous) information about individuals to others.

There is a relatively simple remedy which would go a long way to solving the generic problem. It has the advantage that it is simple to state and easy to understand:

Each time an organization supplies data on an individual to another organization, it must also promptly send TO THE INDIVIDUAL a notice specifying what information was supplied to whom.

Of course, some details need to be added, like requiring that coded information be translated into plain language, and that the criteria used to select the individual for the data transfer be given explicitly (e.g., "We sold a list of all our subscribers with ZIP codes in neighborhoods with median family incomes above \$100,000/year."), but I don't think this would be hard to spell out in a way that would inform the individual without requiring information that the provider doesn't already have.

Since a typical sale results in something being mailed, the cost of mailing the notices ought not to cause a major economic impact.

Jim H.

★ Re: RISKS of unverified driving records (Kabay, RISKS-15.06)

<jhudson@legent.com>
Wed, 6 Oct 93 13:39:32 EDT

Mich Kabay writes:

>Such information is supposedly restricted to "authorized requesters" ...

Veteran RISKS readers probably already know how much damage can be done with the magic three pieces of information (your name, DOB and Social Security number). For newcomers, let me relate a (personally painful) anecdote.

In Massachusetts, the default driver's license number is your Social Security number. In the USA, the default identifying number on your Credit History file is also your Social Security number. 2 years ago, my wallet (with driver's license inside) was stolen. Using the magic three pieces of information which were on the license, some person called TRW Information Services and obtained a copy of my credit history. It cost them \$8. On the credit history was every current credit card number. Armed with the magic three pieces of information plus a credit-card number, the person convinced the credit-card company to change my mailing address. A few days later, the person called and reported the card had been destroyed, and got a new one. Within a week, the person had run up \$8000 in Automated Teller Machine cash withdrawals using the card.

The credit-card company readily admits that their customer-service agent should NEVER have changed the mailing address of the card based on only the magic three pieces of information. However, their security system clearly failed in this case. Having dealt with 6 different credit-card companies during the history of this little affair, I can attest to the fact that the magic three pieces of information are ALL that is needed to pass most companies' security.

Mich goes on to suggest that perhaps we are moving to a "universal identifier". I shudder to think that it could get any MORE universal than NAME+DOB+SS#. What we really need is an authorization scheme that will work for all the copies of our identifiers that are NOT electronic copies.

Jim Hudson < JHudson@legent.com>



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 10

Friday 8 October 1993

Contents

- Wiretap Laws and Procedures **Dorothy Denning**
- Info on RISKS (comp.risks)

Wiretap Laws and Procedures

Dorothy Denning <denning@cs.cosc.georgetown.edu> Fri, 24 Sep 1993 16:49:45 -0400 (EDT)

The following article on wiretap laws and procedures was written in response to the many questions and misunderstandings that have arisen about wiretaps in the context of escrowed encryption as well as Digital Telephony. This article may be distributed. Dorothy Denning denning@cs.georgetown.edu

WIRETAP LAWS AND PROCEDURES WHAT HAPPENS WHEN THE U.S. GOVERNMENT TAPS A LINE

Donald P. Delaney, Senior Investigator New York State Police

Dorothy E. Denning, Professor and Chair Computer Science Department, Georgetown University

> John Kaye, County Prosecutor Monmouth County, New Jersey

Alan R. McDonald, Special Assistant to the Assistant Director Technical Services Division, Federal Bureau of Investigation

September 23, 1993

1. Introduction

Although wiretaps are generally illegal in the United States, the federal

government and the governments of thirty seven states have been authorized through federal and state legislation to intercept wire and electronic communications under certain stringent rules which include obtaining a court order. These rules have been designed to ensure the protection of individual privacy and Fourth Amendment rights, while permitting the use of wiretaps for investigations of serious criminal activity and for foreign intelligence.

This article describes the legal requirements for government interceptions of wire and electronic communications and some of the additional procedures and practices followed by federal and state agencies. The legal requirements are rooted in two pieces of federal legislation: the Omnibus Crime Control and Safe Streets Act (Title III of the Act (hereafter "Title III")), passed in 1968, and the Foreign Intelligence Surveillance Act (FISA), passed in 1978. Title III established the basic law for federal and state law enforcement interceptions performed for the purpose of criminal investigations, while FISA established the law for federal-level interceptions performed for intelligence and counterintelligence operations. We will first describe Title III interceptions and then describe FISA interceptions.

2. Title III Interceptions

Title III, as amended (particularly by the Electronic Communications Privacy Act of 1986), is codified at Title 18 USC, Sections 2510-2521. These statutes provide privacy protection for and govern the interception of oral, wire, and electronic communications. Title III covers all telephone communications regardless of the medium, except that it does not cover the radio portion of a cordless telephone communication that is transmitted between the handset and base unit. The law authorizes the interception of oral, wire, and electronic communications by investigative and law enforcement officers conducting criminal investigations pertaining to serious criminal offenses, i.e., felonies, following the issuance of a court order by a judge. The Title III law authorizes the interception of particular criminal communications related to particular criminal offenses. In short, it authorizes the acquisition of evidence of crime. It does not authorize noncriminal intelligence gathering, nor does it authorize interceptions related to social or political views.

Thirty seven states have statutes permitting interceptions by state and local law enforcement officers for certain types of criminal investigations. All of the state statutes are based upon Title III from which they are derivative. These statutes must be at least as restrictive as Title III, and in fact most are more restrictive in their requirements. In describing the legal requirements, we will focus on those of Title III since they define the baseline for all wiretaps performed by federal, state, and local law enforcement agencies.

In recent years, state statutes have been modified to keep pace with rapid technological advances in telecommunications. For example, New Jersey amended its electronic surveillance statute in 1993 to include cellular telephones, cordless telephones, digital display beepers, fax transmissions, computer-to-computer communications, and traces obtained through "caller-ID".

Wiretaps are limited to the crimes specified in Title III and state statutes.

In New Jersey, the list includes murder, kidnapping, gambling, robbery, bribery, aggravated assault, wrongful credit practices, terrorist threats, arson, burglary, felony thefts, escape, forgery, narcotics trafficking, firearms trafficking, racketeering, and organized crime.

Most wiretaps are large undertakings, requiring a substantial use of resources. In 1992, the average cost of installing intercept devices and monitoring communications was \$46,492. Despite budget constraints and personnel shortages, law enforcement conducts wiretaps as necessary, but obviously, because of staffing and costs, judiciously.

2.1 Application for a Court Order

All government wiretaps require a court order based upon a detailed showing of probable cause. To obtain a court order, a three-step process is involved. First, the law enforcement officer responsible for the investigation must draw up a detailed affidavit showing that there is probable cause to believe that the target telephone is being used to facilitate a specific, serious, indictable crime.

Second, an attorney for the federal, state, or local government must work with the law enforcement officer to prepare an application for a court order, based upon the officer's affidavit. At the federal level, the application must be approved by the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division designated by the Attorney General. At the state and local level, the application must be made and approved by the principal prosecuting attorney of the state (State Attorney General) or political subdivision thereof (District Attorney or County Prosecutor). The attorney must be authorized by a statute of that state to make such applications.

Third, the attorney must present the approved application ex parte (without an adversary hearing) to a federal or state judge who is authorized to issue a court order for electronic surveillance. A state or local police officer or federal law enforcement agent cannot make an application for a court order directly to a judge.

Typically, a court order is requested after a lengthy investigation and the use of a "Dialed Number Recorder" (DNR). The DNR is used to track the outgoing calls from the suspect's phone in order to demonstrate that the suspect is communicating with known criminals.

Title III requires that an application for a court order specify:

- (a) the investigative or law enforcement officer making the application and the high-level government attorney authorizing the application;
- (b) the facts and circumstances of the case justifying the application, including details of the particular offense under investigation, the identity of the person committing it, the type of communications sought, and the nature and location of

the communication facilities;

- (c) whether or not other investigative procedures have been tried and failed or why they would likely fail or be too dangerous;
- (d) the period of time for the interception (at most 30 days extensions may be permitted upon reapplication);
- (e) the facts concerning all previous applications involving any of the same persons or facilities;
- (f) where the application is for the extension of an order, the results thus far obtained from the interception.

The process of making an application for a court order is further restricted by internal procedures adopted by law enforcement agencies to ensure that wiretaps conform to the laws and are used only when justified. The following describes the process for the FBI and the New York State Police.

2.1.1 FBI Applications

In order for an FBI agent to conduct an interception, the agent must follow procedures that go well beyond the legal requirements imposed by Title III and which involve extensive internal review. In preparing the affidavit, the FBI agent in the field works with the field office principal legal advisor and also with an attorney in the local U.S. Attorney's Office, revising the documentation to take into account their comments and suggestions. After the documents are approved by field office management, they are submitted to the Department of Justice's Office of Enforcement Operations (OEO) in the Criminal Division and to the FBI Headquarters (HQ). At FBI HQ, the documents go to the Legal Counsel Division (LCD) and the Criminal Investigative Division (CID). Within the CID, they are sent to the program manager of the criminal program unit relating to the type of violation under investigation, e.g., organized crime. The program manager determines whether the subjects of the proposed interception are worthy targets of investigation and whether the interception is worth doing. Attorneys in the FBI's LCD and the DOJ's OEO further refine the documents.

After the documents are approved by the DOJ's OEO and by FBI HQ, they are referred to the Deputy Assistant Attorney General (or above), who reviews the documents and signs off on them. At this point, the DOJ authorizes the local U.S. Attorney's Office to file the final version of the documents (application, affidavit, court order, and service provider order) in court. The U.S. Attorney's Office then submits the documents and the DOJ authorization to a federal judge. The entire process can take as long as a month.

The following summarizes the people and organizations involved in the preparation or approval of the application and the issuance of a court order:

- 1. FBI agent
- 2. FBI field office attorney (principal legal advisor)
- 3. FBI field office management
- 4. Attorney in local U.S. Attorney's office

- 5. DOJ Office of Enforcement Operations (OEO)
- 6. FBI HQ Legal Counsel Division (LCD)
- 7. FBI HQ Criminal Investigative Division (CID)
- 8. DOJ Deputy Assistant Attorney General (or higher)
- 9. Federal District Court judge

2.1.2 New York State Police Applications

Within the New York State Police, electronic surveillance is conducted by Senior Investigators in the Bureau of Criminal Investigation (BCI). In preparing an affidavit, the investigator works with the District Attorney's Office (or, in the case of a federal investigation, the U.S. Attorney's office) and with the BCI Captain of the investigator's troop. (Wiretap applications can be made and approved by the State Attorney General, but this is unusual.) The Captain assesses whether review by Division Headquarters is necessary and confers with the Assistant Deputy Superintendent (ADS) or Headquarters Captain for final determination. If Headquarters review is deemed necessary, then all documentation is sent to the ADS along with a memorandum, endorsed by the Troop Unit Supervisor and the Troop or Detail Commander, requesting approval. If Headquarters review is deemed unnecessary, then the memo is sent without the documentation. Once the ADS and District Attorney (DA) approve the application, the DA submits the application to a judge who grants or denies the court order.

2.2 Issuance of a Court Order

Not all judges have the authority to grant court orders for wiretaps. In New Jersey, for example, only eight judges are designated as "wiretap judges" for the entire state. These judges are given special training to be sensitive to personal rights of privacy and to recognize the importance of telephone intercepts for law enforcement.

Before a judge can approve an application for electronic surveillance and issue a court order, the judge must determine that:

- (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit an offense covered by the law;
- (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
- (c) normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed or to be too dangerous;
- (d) there is probable cause for belief that the facilities from which, or the place where the communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

In addition to showing probable cause, one of the main criterion for determining whether a court order should be issued is whether normal

investigative techniques have been or are likely to be unsuccessful (criterion (c) above). Electronic surveillance is a tool of last resort and cannot be used if other methods of investigation could reasonably be used instead. Such normal investigative methods usually include visual surveillance, interviewing subjects, the use of informers, telephone record analysis, and DNRs. However, these techniques often have limited impact on an investigation. Continuous surveillance by police can create suspicion and therefore be hazardous; further, it cannot disclose the contents of telephone conversations. Questioning identified suspects or executing search warrants at their residence can substantially jeopardize an investigation before the full scope of the operation is revealed, and information can be lost through interpretation. Informants are useful and sought out by police, but the information they provide does not always reveal all of the players or the extent of an operation, and great care must be taken to ensure that the informants are protected. Moreover, because informants are often criminals themselves, they may not be believed in court. Telephone record analysis and DNRs are helpful, but do not reveal the contents of conversations or the identities of parties. Other methods of investigation that may be tried include undercover operations and stings. But while effective in some cases, undercover operations are difficult and dangerous, and stings do not always work.

If the judge approves the application, then a court order is issued specifying the relevant information given in the application, namely, the identity of the person (if known) whose communications are to be intercepted, the nature and location of the communication facilities, the type of communication to be intercepted and the offense to which it relates, the agency authorized to perform the interception and the person authorizing the application, and the period of time during which such interception is authorized. A court order may also require that interim status reports be made to the issuing judge while the wiretap is in progress.

2.3 Emergencies

In an emergency situation where there is immediate danger of death or serious physical injury to any person, or conspiratorial activities threatening national security or characteristic of organized crime, Title III permits any investigative or law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, or the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof, to intercept communications provided an application for a court order is made within 48 hours. In the event a court order is not issued, the contents of any intercepted communication is treated as having been obtained in violation of Title III.

In New York State, even an emergency situation requires a court order from a judge. However, the judge may grant a temporary court order based on an oral application from the District Attorney. The oral communication must be recorded and transcribed, and must be followed by a written application within 24 hours. The duration of a temporary warrant cannot exceed 24 hours and cannot be renewed except through a written application.

2.4 Execution of a Court Order

2.4.1 Installation of a Wiretap

To execute a court order for a wiretap, the investigative or law enforcement officer takes the court order or emergency provision to the communications service provider. Normally, the service provider is the local exchange carrier. When served with a court order, the service provider (or landlord, custodian, or other person named) is mandated under Title III to assist in the execution of the interception by providing all necessary information, facilities, and technical assistance. The service provider is compensated for reasonable expenses incurred. In light of rapid technological developments including cellular telephones and integrated computer networks, the New Jersey statute also requires the service provider to give technical assistance and equipment to fulfill the court order. This requirement has not yet been tested in court.

Normally, the government leases a line from the service provider and the intercepted communications are transmitted to a remote government monitoring facility over that line. In many cases, the bridging connection is made within the service provider's central office facility. Alternatively, a law enforcement agency may request the service provider to give the "pairs and appearances" (a place to connect to the suspect's line) in the "local loop" for the suspect's phone. A law enforcement technician then makes the connection.

When a suspect's telephone is subject to change (e.g., because the person is attempting to evade or thwart interception), then a "roving" wiretap, which suspends the specification of the telephone, may be used. In this case, prior to intercepting communications, the officer must use some other method of surveillance in order to determine the exact location and/or telephone number of the facility being used. Once determined, the location or telephone number is given to the service provider for coordination and prompt assistance. The officer may not intercept communications randomly in order to track a person (random or mass surveillance is not permitted under any circumstances).

2.4.2 Minimization

Once any electronic surveillance begins, the law enforcement officer must "minimize" -- that is, attempt to limit the interception of communications to the specified offenses in the court order. Prior to the surveillance, a federal or state attorney holds a "minimization meeting" with the investigators who will be participating in the case to ensure that the rules are followed.

Minimization is normally accomplished by turning off the intercept and then performing a spot check every few minutes to determine if the conversation has turned to the subject of the court order. This avoids picking up family gossip. Special problems may arise where criminals communicate in codes that are designed to conceal criminal activity in what sounds like mundane household discussion. If an intercepted communication is in a code or foreign language, and if someone is not reasonably available to interpret the code or foreign language, then the conversation can be recorded and minimization deferred until an expert in that code or language is available to interpret the communication. Should a wiretap fail to meet the minimization parameters,

all of the evidence obtained from the wiretap could be inadmissible.

2.4.3 Recording

All intercepted communications are to be recorded when possible. As a practical mater, law enforcement officers make working copies of the original tapes. In many instances at the state and local level, the originals are delivered to the prosecutor's office and maintained in the prosecutor's custody. The copies are screened by the case officer for pertinent conversations (e.g., "I'll deliver the dope at 8:00 pm."). A compilation of the relevant conversations, together with the corroboratory surveillances often provides the probable cause for search warrants and/or arrest warrants.

2.4.4 Termination of Electronic Surveillance

Electronic surveillance must terminate upon attainment of the objectives, or in any event within 30 days. To continue an interception beyond 30 days, the officer, through a government attorney, must apply for and be granted an extension based upon a new application and court order.

When the period of a court order, or extension thereof, expires, the original tapes must be made available to the issuing judge and sealed under court supervision. The tapes must be maintained in such fashion for 10 years.

2.5 Notification and Use of Intercepted Communications as Evidence

Upon termination of an interception, the judge who issued the court order must notify the persons named in the order that the interception took place. Normally, this must be done within 90 days, but it may be postponed upon showing of good cause. If the judge determines that it would be in the interest of justice to make portions of the intercepted communications available to the subjects, the judge may do so.

The contents of the communications may not be used as evidence in any trial or hearing unless each party has received a copy of the application and court order at least 10 days in advance of the trial, and has been given the opportunity to move to suppress the evidence. A motion to suppress the evidence may be made on the grounds that it was not obtained in complete conformance with the laws.

2.6 Reports

Within 30 days after the expiration or denial of a court order, Title III requires that the judge provide information about the order to the Administrative Office of the United States Courts (AO). Each year the Attorney General (or a designated Assistant Attorney General) must report, on behalf of the federal government, to the AO a summary of all orders and interceptions for the year; reports for state and local jurisdictions are made by the principal prosecuting attorney of the jurisdiction. The AO then integrates these summaries into an annual report: "Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications (Wiretap Report)" covering all federal and state electronic surveillance, including wiretaps. The 1992 report is about 200 pages and includes information about each interception authorized in 1992, update

information for interceptions authorized in 1982-1991, and summary statistics. The summary statistics include the following data (numbers in parenthesis are the 1992 figures):

- (1) number of interceptions authorized (919), denied (0), and installed (846)
- (2) average duration (in days) of original authorization (28) and extensions (30)
- (3) the place/facility where authorized (303 single family dwelling, 135 apartment, 3 multi-dwelling, 119 business, 4 roving, 66 combination, 289 other)
- (4) major offenses involved (634 narcotics, 90 racketeering, 66 gambling, 35 homicide/ assault, 16 larceny/theft, 9 kidnapping, 8 bribery, 7 loansharking/usury/extortion, 54 other)
- (5) average number of (a) persons intercepted (117), (b) interceptions (1,861), and (c) incriminating intercepts (347) per order where interception devices were installed
- (6) average cost of interception (\$46,492)
- (7) type of surveillance used for the 846 interceptions installed (632 telephone, 38 microphone, 113 electronic, 63 combination)
- (8) number of persons arrested (2,685) and convicted (607) as the result of 1992 intercepts
- (9) activity taking place during 1992 as the result of intercepts terminated in years 1982-1991, including number of arrests (1211), trials (280), motions to suppress that are granted (14), denied (141), and pending (37), and convictions (1450) (there is a lag between interceptions, arrests, and convictions, with many arrests and most convictions associated with a wiretap that terminated in one year taking place in subsequent years)

Most of the above data is broken down by jurisdiction. Of the 919 authorized intercepts, 340 (37%) were federal. New York State had 197, New Jersey 111, Florida 80, and Pennsylvania 77. The remaining 114 intercepts were divided among 18 states, none of which had more than 17 intercepts. During the past decade, the average number of authorized intercepts per year has been about 780.

Individual law enforcement agencies also require internal reports. For example, the New York Sate Police requires that each week, the Troop or Detail Captain prepare a report summarizing the status of all eavesdropping activity within the unit, including the productivity and plans for each electronic surveillance installation and a brief synopsis of pertinent activity. This is sent to the New York State Police Division Headquarters Captain who prepares a report summarizing the status of all eavesdropping installations.

One of the reasons for the significant amount of post wiretap reporting is to provide a substantial record for legislatures when considering whether or not to reenact or modify wiretap statutes.

3. FISA Interceptions

Title 50 USC, Sections 1801-1811, the Foreign Intelligence Surveillance Act (FISA) of 1978, covers electronic surveillance for foreign intelligence purposes (including counterintelligence and counterterrorism). It governs wire and electronic communications sent by or intended to be received by United States persons (citizens, aliens lawfully admitted for permanent residence, corporations, and associations of U.S. persons) who are in the U.S. when there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; nonconsensual wire intercepts that are implemented within the U.S.; and radio intercepts when the sender and all receivers are in the U.S. and a warrant would be required for law enforcement purposes. It does not cover intercepts of U.S. persons who are overseas (unless the communications are with a U.S. person who is inside the U.S.). Electronic surveillance conducted under FISA is classified.

FISA authorizes electronic surveillance of foreign powers and agents of foreign powers for foreign intelligence purposes. Normally, a court order is required to implement a wiretap under FISA. There are, however, two exceptions. The first is when the communications are exclusively between or among foreign powers or involve technical intelligence other than spoken communications from a location under the open and exclusive control of a foreign power; there is no substantial risk that the surveillance will acquire the communications to or from a U.S.person; and proposed minimization procedures meet the requirements set forth by the law. Under those conditions, authorization can be granted by the President through the Attorney General for a period up to one year. The second is following a declaration of war by Congress. Then the President, though the Attorney General, can authorize electronic surveillance for foreign intelligence purposes without a court order for up to 15 days.

Orders for wiretaps are granted by a special court established by FISA. The court consists of seven district court judges appointed by the Chief Justice of the United States. Judges serve seven-year terms.

3.1 Application for a Court Order

Applications for a court order are made by Federal officers and require approval by the Attorney General. Each application must include:

- (1) the Federal officer making the application;
- (2) the Attorney General's approval;
- (3) the target of the electronic surveillance;
- (4) justification that the target is a foreign power or agent of a foreign power (except no U.S person can be considered a foreign power or agent thereof solely based on activities protected by the First

Amendment) and that the facilities or places where the surveillance is be directed will be used by the same;

- (5) the proposed minimization procedures, which must meet certain requirements to protect the privacy of U.S. persons;
- (6) the nature of the information sought and type of communications subjected to surveillance;
- (7) certification(s) by the Assistant to the President for National Security Affairs or other high-level official in the area of national security or defense (Presidential appointee subject to Senate confirmation) that the information sought is foreign intelligence information and that such information cannot reasonably be obtained by normal investigative methods;
- (8) the means by which the surveillance will be effected;
- (9) the facts concerning all previous applications involving the same persons, facilities, or places;
- (10) the period of time for the interception (maximum 90 days or, when the target is a foreign power, one year);
- (11) coverage of all surveillance devices to be employed and the minimization procedures applying to each.

Some of the above information can be omitted when the target is a foreign power.

Within the FBI, the process of applying for a court order under FISA is as exacting and subject to review as under Title III. The main differences are that under FISA, the FBI Intelligence Division is involved rather than the Criminal Investigative Division, the DOJ Office of Intelligence Policy and Review (OIPR) is involved rather than either the U.S. Attorney's Office or the DOJ Criminal Division, and the application is approved by the Attorney General (or Acting Attorney General) rather than by a lower DOJ official.

3.2 Issuance of a Court Order

Before a judge can approve an application, the judge must determine that the authorizations are valid; that there is probable cause to believe that the target of the electronic surveillance is a foreign power or agent of a foreign power and that the facilities or places where the surveillance is be directed will be used by the same; and that the proposed minimization procedures meet the requirements set forth in the law. If the judge approves the application, an order is issued specifying the relevant information from the application and directing the communication carrier, landlord, custodian, or other specified person to furnish all necessary information, facilities, and technical assistance and to properly maintain under security procedures any records relating to the surveillance.

3.3 Emergencies

In an emergency situation, the Attorney General or designee can authorize the use of electronic surveillance provided the judge is notified at the time and an application is made to the judge within 24 hours. If such application is not obtained, then the judge notifies any U.S. persons named in the application or subject to the surveillance, though such notification can be postponed or forgone upon showing of good cause.

3.4 Use of Intercepted Communications as Evidence

Like Title III, FISA places strict controls on what information can be acquired through electronic surveillance and how such information can be used. No information can be disclosed for law enforcement purposes except with the proviso that it may only be used in a criminal proceedings under advance authorization from the Attorney General. If the government intends to use such information in court, then the aggrieved person must be notified in advance. The person may move to suppress the evidence.

3.5 Reports

Each year, the Attorney General must give the Administrative Office of the United States Courts (AO) a report of the number of FISA applications and the number of orders and extensions granted, modified, or denied. In 1992, there were 484 orders. Since 1979, there has been an average of a little over 500 FISA orders per year.

Because intercepts conducted under FISA are classified, detailed information analogous to that required under Title III is not reported to the AO, nor made available to the public. However, records of Attorney General certifications, applications, and orders granted must be held for at least 10 years, and the Attorney General must inform two Congressional oversight committees of all surveillance activity on a semiannual basis. These committees are the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

Acknowledgements

We are grateful to Geoffrey Greiveldinger for many helpful suggestions on an earlier draft of this report.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 11

Monday 11 October 1993

Contents

Yet another spacecraft vanishes

Landsat 6

Auto-response missile system

Brian Kenney

Andrew W. Hagen

ITAR issues in PGP & Moby Crypto subpoenas

L. Detweiler

Wiretap Laws and Procedures

Mark Day

David HM Spector

Risks of using phone bill payment systems

Peter A. Grant

Draft Swiss AntiVirus regulation

Klaus Brunnstein

Risks of "security" on Apple Newton

Berry Kercheval

Re: Disrupting Air Traffic Control

Peter B Ladkin

Peter Wayner

Give us all your passwords

Steve VanDevender

Politics is private property in the panopticon society

Jeffrey S. Sorensen

Re: Control Faults cause train crash

Clive Feather

Re: RISKS of unverified driving records

Geoff Kuenning

Libel and Liability for incorrect databases

Terry Gerritsen via Sarah Elkins

Info on RISKS (comp.risks)

Yet another spacecraft vanishes

"Peter G. Neumann" < neumann@csl.sri.com>

Mon, 11 Oct 93 17:34:21 PDT

Landsat 6 was launched on 5 Oct 1993, and had been variously reported as (1) having gotten into an improper orbit, or (2) being in the correct orbit but unable to communicate. The \$228M Landsat 6 has now been declared MISSING. "The object being tracked turned out to be a piece of space junk, officials said." [Source: The San Francisco Chronicle wire services, 9 Oct 1993]

✓ auto-response missile system

Brian Kenney <kenney@hsi.com> Sat, 9 Oct 1993 07:54:45 -0400

The Soviet military constructed a surefire system for retaliating against a U.S. nuclear strike without direct human involvement, and it could still be activated today, a private U.S. expert on nuclear command systems said Friday.

The expert, Bruce Blair, said that once the system is activated by senior Russian military officials, it could automatically send hundreds of nuclear-tipped missiles hurtling towards the United States.

The system would be triggered if automatic sensors - which Blair said may be subject to error - detected a disruption of key military communication links, as well as seismic disturbances, and flashes caused by nuclear detonations inside Russia.

The possibility that Soviet missiles could be launched without specific instruction from nearby military personnel was raised several years ago by Gennadi Pavlov, a retired colonel in the Soviet Strategic Rocket Forces who has spoken at length with Blair.

(Excerpted from The Hartford Courant, 9 Oct 1993.)

The risks are obvious, and horrific.

Russian doomsday machine

"Andrew W. Hagen" <ANDREWH@YANG.EARLHAM.EDU> Sat, 9 Oct 1993 14:49 EST

[Commenting on a variant of the same article, in the Cincinnati Enquirer]

Well, this sure scares me. It's enough that everyone has taken for granted that the danger of massive nuclear war has passed, while nuclear missiles in the former Soviet Union remain pointed at U.S. and Western targets. But now if the software has a few bugs in the code that decides when all Russian military leaders are dead, and it is triggered by some anomaly, then a very serious, huge disaster would follow.

Maybe it's time to start faxing RISKS to the Kremlin.

Andrew W. Hagen andrewh@yang.earlham.edu voice: 317 973-2528 (U.S.)

[All Things Considered covered the same story, as noted by Ken Hoyme, Honeywell Technology Center, Minneapolis, MN, hoyme@src.honeywell.com PGN]

ITAR issues in PGP & Moby Crypto subpoenas

"L. Detweiler" <ld231782@longs.lance.colostate.edu> Wed, 22 Sep 93 21:19:41 -0600

As reported in many places, such as Current Underground Digest, New York Times (Sept 21) and on AP, subpoenas were served on representatives from the companies ViaCrypt and Austin Code Works for materials related to a grand jury investigation in California associated with the U.S. Customs Office. Both warrants are dated 9 Sept., but were served and received two days apart (contrary to the NYT account), with the ViaCrypt on Tues 14 Sept and ACW on Thur 16 Sept:

Austin Code Works:

>Any and all correspondence, contracts, payments, and record,
>including those stored as computer data, relating to the
>international distribution of the commercial product "Moby
>Crypto" and any other commercial product related to PGP and RSA
>Source Code for the time period June 1, 1991 to the present.

ViaCrypt:

>"Any and all

>correspondence, contracts, payments, and records, including those >stored as computer data, involving international distribution related >to ViaCrypt, PGP, Philip Zimmermann, and anyone or any entity acting >on behalf of Philip Zimmermann for the time period June 1, 1991 to the >present."

ViaCrypt just announced publicly a few weeks ago its intent to market a commercial version of PGP. G. Ward, author of Moby Crypto, has been very vocal on various newsgroups (sci.crypt, et. al.) indicating that an NSA agent had previously contacted him over the book, essentially a cryptography tutorial intended to be bundled with disks. Nevertheless the investigation appears at this point to be primarily PGP-oriented based on subpoena wording, and my following comments will focus on that aspect.

If the case progresses beyond this initial inquiry, the issues related to the ITAR code (International Traffic and Arms Regulations) restricting the flow of cryptographic software and documentation long debated in RISKS are likely to receive intense scrutiny and perhaps the first significant judicial test. Many aspects are related to the possibility of ITAR infringement in international PGP distribution, involving highly complex import and export issues, some of which follow.

PGP 1.0 was developed in the U.S. and soon spread internationally after its official release in the month of June 1 1991 (the significance of the subpoena date). Various sections of the ITAR govern the legal export of cryptographic

1

1

2

2

2

2

software and technical documentation, one critical clause defines technical data as follows:

\$120.21 Technical data.

Technical data means, for purposes of this subchapter:

- (a) Classified information relating to defense articles and defense services;
- (b) Information covered by an invention secrecy order;
- (c) Information, in any form, which is directly related to the design, engineering, development, production, processing, manufacture, use, operation, overhaul, repair, maintenance, modification, or reconstruction of defense articles. This includes, for example, information in the form of blueprints, drawings, photographs, plans, instructions, computer software, and documentation. This also includes information which advances the state of the art of articles on the U.S. Munitions List. This definition does not include information concerning general scientific, mathematical, or engineering principles commonly taught in academia. It also does not include basic marketing information or general system descriptions

of defense articles.

The critical question: Is PGP (1) `computer software related to defense' or (2) `technical documentation encompassing general scientific & engineering principles'? Other sections of the ITAR definitely classify cryptographic software as a defense article. In a hypothetical legal case against PGP distribution, the defense might argue that the interpretation of PGP as (2) takes priority over, or is more relevant and applicable, than (1). A wide variety of respondents on the the `cypherpunks' list have indicated that the RSA *algorithm* embodied in PGP is unequivocally public domain knowledge in the U.S. and regularly `taught in academia'.

As a peripheral issue to *export* of PGP above, some sources point out that the IDEA algorithm was implemented outside the U.S. and apparently *imported* into the US in PGP. The legality of this may be affected by sections of the ITAR that bar import of material not legally exportable:

"123.2 Imports.

No defense article may be imported into the United States unless (a) it was previously exported temporarily under a license issued by the Office of Munitions Control; or (b) it constitutes a temporary import/in-transit shipment licensed under Section 123.3; or (c) its import is authorized by the Department of the Treasury (see 27 CFR parts 47, 178, and 179)."

Many armchair-ITAR-experts have noted that the act does not appear to specifically address distribution mechanisms intrinsic to an Internet PGP distribution, specifically either via newsgroups ([x].sources etc.) or FTP. It refers to traditional outlets associated with the "public domain" such as libraries but has questionable, ambiguous, and debatable interpretation on what might be termed `cyberspatial distributions' including BBSes.

Finally, If the case reaches a court, the actual outcome may also hinge on the apparent court precedent that *willful* violation of the ITAR ("criminal intent") must be demonstrated to exist for valid convictions under the law, seen for example in U.S. v Lizarraga-Lizarraga (in 541 F2d 826).

I thank the following people for accounts, information, and analysis which particularly influenced my post (which should in no way be considered representative of their own opinions):

J. Bidzos, G. Broiles, H. Finney, J. Markoff, G. Ward, P. Zimmermann

Note: complete ITAR text can be found via anonymous FTP at ripem.msu.edu:/pub/crypt/docs/itar-july-93.txt.

thanks to M. Riordan and D. Bernstein.

Wiretap Laws and Procedures (Denning, RISKS-15.10)

Mark Day <mday@jukebox.lcs.mit.edu> Fri, 8 Oct 93 23:03:16 -0400

The article by Dorothy Denning et al. reminds me a little of a civics class summary of "How a bill becomes law." Like such a presentation, it was interesting and useful as an introduction to the subject; but I couldn't help feeling that there were probably important "real-world" aspects being omitted. Here are some of my concerns.

1. I was struck by the following statistic about wiretaps in 1992:

number of interceptions authorized (919), denied (0), and installed (846)

No judge saw fit to deny *any* wiretap request that year. I find it difficult to reconcile this statistic with the protections that are enumerated in the report. I think I would feel better if there had been at least a couple of denials out of more than 900 requests. As it is, it seems as though either the judges aren't really filtering requests carefully, or the agencies aren't presenting any cases that are marginal.

- 2. I am unconvinced by the rationale for having only a select set of judges hearing wiretap requests. I would worry that having one judge hear multiple wiretap requests probably encourages the review process to become routine: "this request is just like the one you approved last week, so just issue the court order, please."
- 3. Knowing that "the entire process can take as long as a month" is not nearly as interesting as knowing how *fast* the entire process can happen.
- 4. Being at least vaguely aware of some cases when people in law

enforcement agencies have placed unauthorized wiretaps, I would be interested in knowing how often people have actually been tried and convicted of those offenses. Simply knowing what the law says is useful, but one also needs a sense of how well the law is enforced.

--Mark Day mday@lcs.mit.edu

✓ Wiretap practices and procedures (Denning, RISKS-15.10)

<spector@jpmorgan.com>
Sun, 10 Oct 1993 19:57:06 -0400 (EDT)

Although the article by Dr. Denning et al. is very interesting and enlightening on the subject of _legal_ wiretaps, it would seem however that she and others continue to miss the most important issue involved in the key-escrow/cryptography debate. That being the fact that the citizenry has absolutely NO ASSURANCE that the ability to monitor communications will not be used in an extra-legal fashion.

The last 30 years of history (for starters) are rife with de-facto, documentable, pervasive violations of the rights of individuals by a government that has used the ability to tap/monitor/intercept or otherwise spy on individuals outside of the bounds of what-ever wiretap laws are in effect with impunity.

Some small examples perhaps? Watergate, Dr. Martin Luther King and other members of the Civil Rights Movement, Groups opposed to the wars in Viet Nam, Central America, and elsewhere, Anti-nuclear activists... Need I go on?

Arguments that "good choices" for the escrow agents will end this problem border on insulting.

Perhaps Dr. Denning could explain how we can be assured this power will not be abused in this fashion? Perhaps a guide to "What happens then the US Government ILLEGALLY taps a line?"

David HM Spector Spector David@JPMORGAN.COM

These opinions are my own, and do not in any way represent my employer...

Risks of using phone bill payment systems

"Peter A. Grant" <grant@erich.triumf.ca> Fri, 08 Oct 1993 23:54:52 PST

Well, I've finally been bitten by a banking system, other than the standard ATM problems. Our local credit union just started a phone-based bill payment system to add to their system which allows one to check balances, transfer funds, list cleared entries, etc.

I signed up and thought it was wonderful for the first month. This month all seemed to go well, but a couple of days after paying all three phone bills and a MasterCard bill, I found a message on our answering machine from VanCity asking one of us to give them a call. I was positive that I hadn't bounced a cheque, so I phoned.

It turns out that when I paid on of my phone bills, the confirmation number that I was given by the automated system wasn't unique after all and when the batch processing took place later that day only the first transaction with that identifier was actually carried out. I got to hear about it three days later - two days after the due date. "A work request has been filled in to look into this problem" was what I was told. I phoned in another transaction as soon as I hung up, and am hoping that one went through and that some magic will prevent me from finding a late payment charge on next month's bill.

Just when you thought it was safe to use sequence numbers, eh?

Peter Grant Database and Systems Administration, Controls Section, TRIUMF "Canada's National Meson Facility" grant@triumf.ca

Draft Swiss AntiVirus regulation

Klaus Brunnstein

Sat, 9 Oct 1993 13:49:29 +0100

To whom it may concern:

The Swiss Federal Agency for Informatics (Bundesamt fuer Informatik, Bern) is preparing a legislative act against distribution of malicious code, such as viruses, via VxBBS etc. You may know that there have been several attempts to regulate the development and distribution of malicious software, in UK, USA and other countries, but so far, Virus Exchange BBS seem to survive even in countries with regulations and (some) knowledgeable crime investigators.

In order to optimize the input into the Swiss legal discussion, I suggested that their draft be internationally distributed, for comments and suggestions from technical and legal experts in this area. Mr. Claudio G. Frigerio from Bern kindly translated the (Swiss) text into English (see appended text, both in German and English); in case of any misunderstanding, the German text is the legally relevant one! Any discussion on this forum is helpful; please send your comments (Cc:) also to Mr. Claudio G. Frigerio (as he's not on this list).

"The Messenger" (Klaus Brunnstein: October 9, 1993)

Entwurf zu Art. 144 Abs. 2 des Schweizerischen Strafgesetzbuches

"Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder uebermittelte Daten loescht, veraendert oder unbrauchbar macht, oder Mittel, die zum unbefugten Loeschen, Aendern oder Unbrauchbarmachen solcher Daten bestimmt sind, herstellt oder anpreist, anbietet, zugaenglich macht oder

Appendix 1:

sonstwie in Verkehr bringt, wird, auf Antrag, mit der gleichen Strafe belegt."

P.S.: gleiche Strafe =JBusse oder Gefaengnis bis zu 3 Jahren; bei grossem Schaden, bis zu 5 Jahren Gefaengnis sowie Verfolgung von Amtes wegen (Offizialdelikt)

Draft of article 144 paragraph 2 of the Swiss Penal Code (English translation)

Anyone, who, without authorization

- erases, modifies, or destructs electronically or similarly saved or data, or anyone who,
- creates, promotes, offers, makes available, or circulates in any way means destined for unauthorized deletion, modification, or destruction of such data,

will, if a complaint is filed, receive the same punishment.

P.S.: same punishment = fine or imprisonment for a term of up to three years; in cases of a considerable dam-age, five years with prosecution ex officio.

Author: Claudio G. Frigerio, Attorney-At-Law, Swiss Federal Office of Information Technology and System, e-mail: bfi@ezinfo.vmsmail.ethz.ch

✓ Risks of "security" on Apple Newton (Siebert, RISKS-15.09)

Berry Kercheval <kerch@parc.xerox.com> Mon, 11 Oct 1993 13:34:45 PDT

It's even worse: apparently the password must be stored in the Newton's in-memory dictionary, or the handwriting recognizer will refuse to recognize the password!

To be fair, you *can* instruct the Newton to recognize words not in its dictionary, but then there is another set of problems getting it to accept what you write.

--berry

Re: Disrupting Air Traffic Control (Marshall, RISKS-15.09)

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 9 Oct 93 00:28:39 BST (Sat)

The report misstates what must have happened.

- > [The couple in the Cessa 150] forgot to turn off their transmitter and
- > broadcast their moments of passion to air traffic controllers

To talk on a radio frequency, it is necessary to depress, and to maintain depressed, the 'talk' button either on a microphone or on the horn of the

control column. The condition reported in the note above is a 'stuck mike', in which release of the button does not terminate the transmission as it should. Stuck mikes happen infrequently, although all moderately experienced pilots have heard them. The Cessna pilot was not the cause of this abnormal condition, neither can he be held particularly responsible for not detecting it. He *may* be held responsible for not flying with due care and attention, under the presumption that one cannot effectively make love and fly at the same time, but proving that would be hard (how does the CAA know that it wasn't just a tape on his stereo?).

If one is alert, then one might notice that radio traffic was abnormal, and use the radio to query ATC (`Edinburgh Control, how do you read?'), thereby (usually) `unsticking' the mike. This happens less frequently in my experience than the case in which the mike just unsticks itself (I've never had a stuck mike myself that I've noticed).

I don't see what any of this has to do with the subject matter of RISKS. It's another example of amusing but misleading journalism.

Peter Ladkin

★ Re: Risks of disrupting air traffic control ("Mile High Club")

Peter Wayner <pcw@access.digex.net> Sat, 9 Oct 1993 22:55:20 -0400

>The couple, flying in a private Cessna 150 plane near the Scottish city of >Edinburgh, began by debating whether they should have sex 5,000 feet (1,500 >metres) above ground and join the "Mile High Club." Their conversation grew >more and more passionate and then ceased.

Of course, the real RISK here relates to a mile being 5280 feet, which is about three or four feet more than *1600* meters.

If another plane was at 5000 feet, a near Miss would not be as good as a smile.

-Peter Wayner

✓ give us all your passwords

Steve VanDevender <stevev@miser.uoregon.edu> Sun, 10 Oct 93 00:59:16 PDT

Last week, many of us at the company where I work were astonished to receive an e-mail message from our parent company's legal department asking everyone to send them all the passwords everyone had used on our LAN servers since January, 1991, except for current passwords. Fortunately, it was shortly revealed that this did not apply to our division, but not before I had sent back a reply telling the person in the legal department how dangerous I thought this was.

Later we found out at a company meeting that another division in our family of companies is being sued because of some possibly suspicious stock trading, and our legal department wants to make sure that it can get at any records on their network servers. I, of course, suspect that they are being spectacularly ignorant of how little use the password lists would be to them and the security risks involved with having lists of individual passwords laying around in plaintext form. Even though none of the passwords should be current, my experience suggests that many people stick to certain themes and patterns for passwords, especially when password aging is used, as it is on our servers. Our passwords expire every 40 days, which means that everyone working at our company since January 1991 has gone through 25 passwords by now, giving any crackers a sizable database to extrapolate from. And of course, everyone will probably send their password lists by e-mail, giving crackers an easy opportunity to intercept such lists.

politics is private property in the panopticon society

Jeffrey S. Sorensen <sorenjs@pb.com> Mon, 11 Oct 93 10:38:53 -0400

The _New Haven Register_ had an AP story about the probe into the industrial spying performed by a group of cable system operators. This spying included surveilance, tracking down license plates and investigating long-distance call records. According to the cable companies all of this was done using publicly obtainable information.

The money involved in the deals between cable and television has driven the cable companies to use such tactics because they are afraid that regulators are fraternizing with telephone company executives.

I can almost see William Gibson's vision of the future unfolding before my eyes. I also see democracy being ground between the gears of industry and government. (Perhaps I should also mention the three part series of articles in _In These Times_ on the new pseudo-grass roots lobbying firms that sell the line "How many angry constituents do you want calling your legislators each day? Name your price.")

According to the article, a company called _Scanners_ out of Denver will "fax a list of toll calls made by anyone, anywhere, for up to \$125." (No doubt the company takes their name from the movie about people who make your blood boil and your veins pop out on your head.) It seems that while the content of calls is private and cannot be monitored without a court order, the billing information is not protected.

The larger problem is that our law currently only provides us with a modicum of protection when we have a "reasonable expectation of privacy." At the same time, it is becoming increasingly clear that no reasonable person can ever expect to have any privacy. I wish that someone in the news media would get our legislators to WAKE UP by publishing a complete list of the legislators' calls. It worked in the Bork/Video-tape rental records case (or at the very least, a law addressing this was put on the books; I'm not sure it's enforced.)

Jeffrey Sorensen sorenjs@pb.com

Re: Control Faults cause train crash (Winter, RISKS-15.09)

Clive Feather <clive@x.co.uk> Mon, 11 Oct 93 16:55:09 BST

> Moreover, he has to take control on the station (Canary Wharf) the software > is not yet able to deal with after all those years of operation.

The conductor does not have to take control at Canary Wharf. What is happening is that the section from West India Quay to Canary Wharf is under reconstruction, and the control software, rather than being edited once a week, is set to be *extremely* conservative in its driving habits over this section. Most conductors would rather use the manual controls for this short section rather than delay the train.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford, WD1 8YN, United Kingdom clive@sco.com Phone: +44 923 816 344

★ Re: RISKS of unverified driving records (Hudson, RISKS-15.09)

Geoff Kuenning <geoff@FICUS.CS.UCLA.EDU> Mon, 11 Oct 93 11:04:42 -0700

Jim Hudson writes:

- > The credit-card company readily admits that their customer-service agent
- > should NEVER have changed the mailing address of the card based on only the
- > magic three pieces of information. However, their security system clearly
- > failed in this case.

I recently moved, and took the "easy way out" in several cases by filing my change of address by telephone. I was pleased to note that several companies sent me a followup letter of the form "we recently processed your address change; please contact us if this is incorrect." Unfortunately, in every case they sent the letter only to the *NEW* address! Duuuuhh. How about sending it to both the old and new locations, guys? Oh no, we wouldn't want to spend that extra 29 cents on postage.

Geoff Kuenning geoff@maui.cs.ucla.edu geoff@ITcorp.com

Libel and Liability for incorrect databases

<Sarah_M._Elkins.Wbst139@xerox.com>
Mon, 11 Oct 1993 12:27:15 PDT

I got the following extract, supposedly from the "Lawyers Weekly", a UK publication I guess (can anyone with more information access verify this, or better, verify the account below?), on a jokes distribution a few weeks back. I know some aspects of libel laws are stricter there than in the U.S., but still wonder if some variant might be used to force information distributors (credit agencies, etc.) to correct their databases sooner, or even hold them liable for incorrect information in the first place.

Sarah (elkins.wbst139@xerox.com)

>From: ember!vicuna@math.uwaterloo.ca >From: terry@gtm-inc.com (Terry Gerritsen)

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)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 12

Thursday 14 October 1993

Contents

- Networking on the Network Phil Agre
- Info on RISKS (comp.risks)

Networking on the Network

Phil Agre <pagre@weber.ucsd.edu> Wed, 13 Oct 1993 17:57:14 -0700

The following article (about 6300 words and 40kB) is a how-to for research people who are learning to use the Internet as part of their professional networking. It has two goals, practical and philosophical:

Its practical goal is to give new users a structured way of thinking about e-mail as part of everyday life. It warns against some of the more common risks of indiscriminate e-mail use, and it offers some specific formulas for approaching common situations.

Its philosophical goal is to cast doubt on the idea of "virtual communities" and "cyberspaces" that are supposed to exist in a different dimension from the rest of our lives. To the contrary, I think we should learn to view electronic communications as part of a larger ecology of communication media and community-building processes. That's not to say that e-mail has no revolutionary potentials; quite the contrary, it is to emphasize that real revolutions can be made, and can *only* be made, as the article says, "down here on earth, amidst your actual relationships with actual people, and not in an abstract technological head-space."

"Networking on the network" is also an experiment in Internet publishing. I don't get any credit for it at tenure time, but I do get to keep revising it forever, based on the comments I receive from people all over the net. At any given time the current version can be fetched by sending an e-mail message like so:

To: rre-request@weber.ucsd.edu Subject: archive send network

So please do send me any comments you might have. I'm especially hoping to get comments from students in classes (of which there are several already) in which "Networking on the network" is assigned as a reading. Phil Agre, UCSD

NETWORKING ON THE NETWORK

Phil Agre
Department of Communication D-003
University of California, San Diego
La Jolla, California 92093-0503

pagre@ucsd.edu

Version of 21 September 1993.

Copyright 1993 by the author. You may forward these notes electronically to anyone for any non-commercial purpose. Please send me any comments that might help to improve future versions.

The Internet and other digital networks are currently undergoing explosive growth. Several million people employ electronic mail for some significant portion of their professional communications. Yet in my experience few people have figured out how to use the net productively. A great deal of effort is being put into technical means for finding information resources on the net, but hardly anybody has been helping newcomers figure out where the net fits in the larger picture of their own careers. These notes are a first crude attempt to fill that gap, building on the most successful practices I've observed in my fifteen years on the net. Although I will focus on the use of electronic communication in research communities, the underlying principles will be applicable to many other communities as well. Everyone's life is different, cultures and disciplines have their own conventions, and it's all just my opinion anyway, but perhaps my suggestions will be useful. Do not interpret them as a set of rules or a manual of etiquette or morality, but rather as a resource in figuring out your own personal way of getting around in your particular professional world. And definitely do not turn them into any kind of ersatz social identity or value system. Instead, make sense of them within some larger set of values that you develop as you live your life.

The first thing to realize is that net-world is part of reality. The people you correspond with on the network are real people with lives and careers and habits and feelings of their own. Things you say on the net can make you friends or enemies, famous or notorious, included or ostracized, respected or scorned. You need to take the electronic part of your life seriously. In particular, you need to think about and consciously choose how you wish to use the network. Regard electronic mail as part of a larger ecology of communication media and genres: telephone, archival journals and newsletters, professional meetings, paper mail, voice mail, chatting in the hallway, lectures and colloquia, job interviews, visits to other research

sites, and so forth, each with its own attributes and strengths. The relationships among media will probably change and new genres will probably emerge as the technologies evolve, but make sure that you don't harbor the all-too-common fantasy that someday we will live our lives entirely through electronic channels. It's not true.

One might engage in many different professional activities over the net: sharing raw data, arguing about technical standards, collaborating on research projects, commenting on drafts of papers, editing journals, planning meetings and trips, and so on. Underlying all of these disparate activities, though, is the activity of building and maintaining professional relationships. All of the capacity and velocity of electronic communication is wasted unless we use it to seek out, cultivate, and nurture relationships with other human beings. Unfortunately the existing mechanisms for electronic interactions, by seeming to reduce people to abstractions and codes (like "c2nxq@loco.thrust.com"), make it difficult to keep this deeper dimension of interaction in mind. Still, there's no escaping it: if you aren't consciously building relationships, you're probably getting lost.

At the most fundamental level, then, most of my advice has nothing intrinsically to do with electronic communication at all. My real topic is not (technological) networks but (professional) networking. Therefore I'll discuss networking in a general way before describing how electronic mail can accelerate it.

In the past, the only ways to learn networking were to be born to a socially well-connected family or to apprentice yourself to a master of the art.

And even though the term "networking" became fashionable during the 1980's, it is only recently that decent books on the subject have begun to appear.

(Some of these are listed in the appendix.) Many people resist the idea of networking because they associate it with the greasy connotations of "knowing the right people", because of a distaste for "politics", because they've learned that useful knowledge about how the world works is necessarily "cynical", or because it supposedly takes time away from "getting real work done". Even when the practical skills of networking are explicitly taught, it is usually done over coffee or beer, in hushed tones, as if there were something illicit about it. Indeed, many people will accuse you of all sorts of terrible things if you admit to having worked-out ideas on the subject. I couldn't disagree more.

The truth is that the world is made of people. People out of communities are like fish out of water or plants out of soil. Research of all kinds depends critically on intensive and continually evolving communication among people engaged in related projects. Networking cannot substitute for good research, but good research cannot substitute for networking either. You can't get a job or a grant or any recognition for your accomplishments unless you keep up to date with the people in your community. Establishing professional relationships with particular people and involving yourself in particular professional communities will change you: not only will you internalize a variety of interesting points of view, but you will become more comfortable in your writing and speaking because you will be engaged in an ongoing conversation with people you know. And if no community is waiting for you, you will have to go out and build one -- one person at

a time. This "overhead" can be a nuisance at first, but none of it is terribly difficult once you get some practice and really convince yourself that you cannot sustain your professional life without devoting about a day per week to it.

Here, then, are some of the fundamentals of professional networking. They will sound cumbersome and abstract. You'll be able to skip some of the steps as you get established in your field (or if, unlike most of us, you are able to charm rooms full of strangers in twenty minutes), but if you're starting from zero then the process really is this complicated:

- (1) Know your goals. Getting tenure? Being invited to conferences in Europe? Filling your life with intelligent conversation? Developing leadership skills? Clear goals will help you maintain focus. Do not, however, use your professional networking to achieve personal goals such as finding friends and lovers. It's just great when professional relationships happen to develop into personal relationships (assuming that you're clear about the conflicts of interest that professional power differences can bring), but always keep in mind that professional relationships and friendships are different sorts of things, no matter how friendly they might seem on the surface.
- (2) Identify some relevant people. Awful as it might sound, "relevance" here is reckoned in functional terms: given how your particular professional world operates, with whom do you have a mutual interest in making contact? In the world of research, mutual interest is almost always defined through the content of your research: you wish to contact people whose research bears some important relationship to yours. This is the case I will assume here. How do you identify these people? Most of the methods are wholly mundane: asking people with good networks, chance mentions of people in conversation, and habitually scanning bibliographies, abstracts, and conference proceedings. Get used to these mundane practices before you explore anything fancier.
- (3) Court these people individually. The right way to do this is not entirely obvious. Unless you are already well known in the person's field, you should NOT simply approach them and say, "hey, I hear you're interested in XXX". The reason for this is profound, viz, whereas ordinary social life calls on you to simply be yourself in this way, professional life calls on you to construct and maintain a complex professional persona that is composed largely of your research, writing, and professional activities. Therefore, in approaching possible professional contacts, you should let your research articles be your emissaries. (If you haven't written anything yet, let your networking wait until you have. Unpublished articles, conference papers, and research reports are all okay. In writing your first articles, you will want to lean heavily on your local system of advisors, mentors, and peers; the skills involved in this process are a subject for another time.) Here is the procedure: (a) choose someone you wish to approach; (b) make sure that your article cites that person's work in some substantial way (in addition to all your other citations); (c) mail the person a copy of your article; and (d) include a low-key, one-page cover letter that says something intelligent about their work. If your work and theirs could be seen to overlap, include a concise statement of the relationship you see between them. The tone of this letter counts.

Project ordinary self-confidence. Refrain from praising or fawning or self-deprecating or making a big deal out of it. And don't drop dead if you don't get a reply right away. Anybody who isn't wholly egotistical or seriously famous will appreciate your taking the trouble to write them. In my experience, most everyone in the world of research is desperate for someone to actually understand what they're saying. If they don't reply, the most likely reason is laziness. (Warning: Do not use citations as a form of flattery. This sort of thing fools nobody. Instead, think of a research paper as a kind of open letter, with the people you cite included in its addressees. Research is a conversation, and your paper is a way of starting new conversations with people in your area. When in doubt, get advice.)

- (4) Meet this person face-to-face at a professional meeting. Unless you really know what you're doing, you should keep the conversation to safe, professional topics. Ask them intelligent questions about their work. Ask them about the people they work with. Figure out who you know (that is, professionally) in common. If other people, projects, or laboratories come up in the conversation, say whatever positive things you honestly have to say about them -- avoid criticism and negativity. If the person is significantly more powerful than you then the prospect of this conversation will probably make you uneasy. That's okay. Concentrate on meeting people who don't intimidate you and your courage will grow. Your single most important audience is actually not the power-holders of your field but rather the best people of your own generation. These people share your situation and will usually be happy to talk to you. Nonetheless, you should always give full and respectful attention to anybody who approaches you, no matter how junior or marginal they might be. If you find yourself talking to a space cadet or a jerk, have compassion. It's up to you which relationships to pursue in depth, but everyone you meet shapes your reputation -- and justly so. It really is imperative that you conduct your professional activities ethically -- and not just within the bounds of a legalistic interpretation of ethical principles, but with an active and creative solicitude for the well-being of the individuals and communities around you. You don't have to be shy or let people walk on you, but if you get ahead at the expense of others then it will catch up with you -- in your heart if not immediately in your paycheck.
- (5) The next step, I'm afraid, depends on the hierarchy. If someone is qualitatively more senior than you, your goal is simply to get on their radar screen -- one chat per year is plenty. (That's mostly because they already have a full network and have begun to reckon relevance differently from you.) If someone is more or less equal to you in the hierarchy, and if they still strike you as relevant, worthwhile, and trustworthy, it will probably be time to exchange pre-publication drafts of new articles. Again, keep it low-key: pass along a draft that you're ready to circulate and invite "any comments you might have". Upon receiving such a draft yourself, take the trouble to write out a set of comments on it. Make sure your comments are intelligent, thoughtful, constructive, and useful. If you are uncomfortable writing critical comments, frame them with positive comments ("this is obviously an important topic and you've made some valuable observations"), develop a lexicon of hedges ("I'm not clear on ...", "maybe"), emphasize what's possible instead of what's wrong ("maybe you can

build on this by ...", "perhaps you can further clarify this by ..."), and keep to specifics ("how does this step follow?" as opposed to "woolly and vague"). This draft-exchanging ritual is tremendously important, but nobody ever seems to teach you how it's done. When in doubt, ask for help. And if somebody comments a draft for you, thank them and be certain to reciprocate (and don't forget to include them in the acknowledgements section of the finished paper). Doing so, even once, will almost certainly cement a long-term professional relationship -- a new member of your network.

(6) Follow up. Keep coming up with simple ways to be useful to the people in your network. A few times a year is plenty. Pass things along to them. Mention their work to other people. Plug them in your talks. Include them in things. Get your department or laboratory to invite them to speak. Put them up when they come to town. And invent other helpful things to do that nobody ever thought of before. None of this is mandatory, of course, but it helps. And I can't repeat this often enough: keep it low-key. Never, ever pressure anybody into anything. Never heap so much unsolicited help on someone that they feel crowded or obligated. Don't complain. And furthermore, make sure you're doing all this stuff from courtesy and respect, and not as any kind of phony politicking -- people can spot phonies a mile off. Build relationships with personal friends outside of work so you won't be unconsciously trying to get professional contacts to play roles in your personal life (for example, the role of sounding board for your troubles). If you don't hear from someone for a while, let it ride. If you feel yourself getting obsessive about the process, go talk it out with someone you regard as wise.

This step-by-step procedure is obviously oversimplified and somewhat rigid. And it omits many topics, such as the claims that effective networking makes on numerous other activities: giving talks, mixing at receptions, formulating research results, choosing where and when to publish, organizing workshops and journal issues, and so forth. Nonetheless, some basic points about the networking process should be clear enough:

- * It takes time -- you have to be patient and let it happen.
- * It focuses on particular individuals and particular relationships.
- * It produces bonds of reciprocal obligation through the exchange of favors.
- * It calls for a significant but manageable up-front investment.
- * It requires you to cultivate a realistic awareness of power.
- * It involves a variety of communication media.
- * It forces you to develop communication skills in each of these media.

These statements, of course, aren't etched in stone. You should keep reflecting on your professional life as you go along, continually trying to come up with a better way of explaining it to yourself. No doubt I've left out some important dimensions of the process.

Having surveyed the basics of networking and professional relationships,

it's time to consider the role that electronic communication can play. The most important thing is to employ electronic media consciously and deliberately as part of a larger strategy for your career. It's okay to use the net in other parts of your life: hunting for people to correspond with, organizing political movements, joining discussions of sex and child-rearing, and so forth. But so long as you have your professional hat on, every message you exchange on the network should be part of the process of finding, building, and maintaining professional relationships. I cannot emphasize this strongly enough, because electronic mail seems to provide endless temptations to the contrary. I succumb to these temptations regularly, and I invariably regret it. They include:

- * The temptation to react. Most on-line discussion groups consist largely of people reacting to things they've seen, acting on impulse without thinking through their own agenda in the situation. (One kind of reacting is called "flaming", but many other kinds of reacting are equally insidious.) E-mail encourages this kind of reactive behavior by making it easy to respond to a discussion with only a few rapid keystrokes. Keep your cool. The more impulsive you are, the more you're using the network to find friends as opposed to colleagues, and the greater your unmet needs for affirmation and attention, the more you will be led into reaction. One slip-up will not bring your career to a halt, but you should definitely be aware of the phenomenon.
- * The temptation to pretense. Electronic communication affords the illusion of semi-anonymity: since people only know you by your mailbox address, you tend to lose the inhibitions that normally keep you from pronouncing on matters that you are not really informed about. The chatty informality of most e-mail discussion groups, which is certainly capable of being a force for good in the world, nonetheless also tends to wear down these inhibitions. Besides, everyone else is doing it. But pretending to know things is just as bad an idea on e-mail as it is face-to-face. Keep focused on your own unique professional contributions and let the random chatter slide. Beware: many people revile this injunction against pretense, based on a false conception of community and a misguided fear of elitism. I am certainly not promoting the reign of experts here; I am simply applying to electronic communication the everyday injunction to know what you're talking about.
- * The temptation to paranoia. Along with your own anonymity goes the frequent difficulty of knowing who exactly is receiving your discussion-group messages. As a result, many people just listen in, terrified to say anything for fear that they will be dumped on by powerful experts. This problem is not exclusive to e-mail, of course, but it is quite real. The solution is to focus on the careful, step-by-step process of approaching individuals, leaving group participation until you feel more comfortable -- which you will, eventually.
- * The temptation to get overwhelmed. It's easy to sign up for everything that sounds interesting, or to pursue dozens of people in every direction, only to find yourself swamped with messages to read and favors to return. If you're getting more than about twenty messages a day in your mailbox then you should probably review your goals and prune back accordingly.

- * The temptation to get addicted. Addiction means getting overwhelmed on purpose. It's tremendously common. The test is, can I just decide to give it a rest for a few days?
- * The temptation to waste time. Exploring the net is a tremendous way to avoid writing your thesis. It goes on forever these days, and you can waste a great deal of time playing with it. Unfortunately, random exploration will rarely yield network information resources that are actually useful to your real career goals. Useful information is always bound up with useful people. Therefore, your explorations of the network will most usefully be guided by your goals and structured by the search for people to add to your network. If you really do care about on-line information resources, develop a good relationship with a librarian. Librarians are almost uniformly wonderful people who enjoy helping you find things, whether on the net or elsewhere. (If you're shy about asking people to do things for you, instead tell them what you're trying to accomplish and ask them for advice about how to do it yourself and for suggestions about who might be able to help you.)
- * The temptation to blame e-mail for your problems. If you're a beginner with electronic communication, you will probably have a few mishaps at some point: getting put down by somebody, acting on an impulse that you later regret, inadvertently sending a message to the wrong person, violating the obscure protocols of professional communication, getting overwhelmed with marginally worthwhile messages, finding yourself trapped in long, complicated correspondences, or whatever. When this happens, you might be moved to blame the medium; you'll find yourself saying that e-mail is dangerous or worthless or overwhelming. But ask yourself: do similar things happen in group meetings or conferences or over the telephone or in paper mail? E-mail has its shortcomings to be sure, but it's just a tool like any other. You'll have to learn how to use it, what to use it for, and when not to use it.

Of course, a little messing around won't kill you. And it's just as bad to go to the opposite extreme and become a compulsive machine for scoring points and making connections. What matters is understanding whatever you're doing within the bigger picture of your life and career.

So, assuming you've been duly admonished against these temptations, what ARE the most constructive uses of electronic communication? Let's review the six-step networking process I outlined above and look for opportunities to use electronic mail to ease the various steps:

- (1) Know your goals. Electronic mail can't help you much here. Indeed, you'll need to make sure that your goals are not defined narrowly in terms of electronic mail. Once you've begun corresponding with people you consider wise, you can begin to seek advice from them. Asking for advice is an art in itself, and other things being equal it's best done face-to-face, but once you know someone fairly well on a face-to-face basis you can move some of the discussion to e-mail.
- (2) Identify some relevant people. Listening in on discussion groups is one way of finding relevant people, especially the ones who aren't so famous. If someone in a discussion impresses you, fight the temptation to

approach them right away. (It's obviously okay to answer routine functional requests on the order of, "does anyone know ...?", provided you simply answer the request and leave the networking for later.) Instead, consult your library's card catalog and periodical indexes (which are probably on-line anyway), look the person up, read a sample of what they've written, and proceed with the next step. Only if you cannot find any relevant publications should you consider sending them a concise note saying, "what you said about XXX is interesting to me because of YYY; if you have an article on the subject ready to distribute then I'd much appreciate a copy". Having listened in on a discussion group for a while and observed its customs and conventions, you might then consider contributing something yourself. Don't just react or chat. Instead, write a really intelligent, self-respecting, unshowy, low-key, less-than-one-page message that makes a single, clearly stated point about a topic that's relevant to both their interests and your own, preferably but not necessarily as a contribution to an ongoing discussion. Sit on this message overnight to make sure you're not just reacting to something or repeating a familiar point that happens to make people in your community feel good. If you're feeling uneasy or compulsive about it then get comments from someone close to you whose judgement you trust. Having thus refined your message, contribute it to the discussion group and see what happens. If nothing happens, don't sweat it. If it starts a discussion then listen respectfully, constructively acknowledge all halfways worthwhile responses, and be sure you're not just reacting to things. This process might flush out some people worth adding to your network. Or it might not. In any case it will get your name out and will, with remarkable efficiency, establish your reputation as an intelligent and thoughtful person. Remember: don't bother doing any of this until you've written up some work and are ready to actually start building your network.

- (3) Court these people individually. In the old days, the article and letter you sent to approach someone were both printed on paper. Should you use electronic mail instead? I actually recommend using paper. At least you shouldn't use electronic media just because they're fun. For one thing, paper is much easier to flip through quickly or to read on the subway. It's also much easier to write comments on. Use your judgement. If you do decide to employ electronic mail for this purpose, use just as much care as you would on paper. Remember that first impressions count. And don't try to use e-mail for the get-to-know-you type of chatting that should logically follow at this point. Instead ...
- (4) Meet this person face-to-face. I believe firmly, despite all the talk about "virtual reality" and "electronic communities", that electronic communication does not make face-to-face interaction obsolete. Instead, as I said at the outset, you should think of e-mail and face-to-face interaction as part of a larger ecology of communication media, each with its own role to play. In particular, I honestly believe that you do not really have a professional relationship with someone until you have spoken with them face-to-face at length, preferably in a relaxed setting over a social beverage. Call me old-fashioned if you will, but make sure that any aversion you might have to face-to-face interaction isn't based on inertia or fear. Inertia and fear are normal feelings, but they have to be worked through and faced. Having said that, the availability of e-mail will

nonetheless bring subtle changes to the ecology of communication in your field. This is particularly true with regard to the telephone, whose uses change considerably in e-mail-intensive communities -- so much so, in fact, that many people nearly stop using the phone altogether (or never learn how) and try to use e-mail for unsuitable purposes like asking discussion groups for information that could have been gotten more easily through resources listed in the front of the phone book. (It's amazing what you can accomplish over the telephone once you learn how.) But the role of face-to-face interaction will change as well, particularly since many kinds of routine work can be conducted almost as easily at a distance electronically as in formal meetings face-to-face. Electronic communication might even allow face-to-face interaction to shift its balance from its practical to its ritual functions. In any case, the general lesson is to pay attention to the relationships among media so you can use the right tool for each job. One more note: when you go to a professional meeting, take a minute to flip through your e-mail correspondence and make a list (ideally on paper) of all the people you've "met" on-line who might attend the conference. Few things are more embarrassing than drawing a blank when someone at a conference approaches you and tries to pick up a conversation begun on e-mail.

- (5) Exchange drafts. Once again, you should decide whether to use paper or electronic mail to exchange drafts of articles. My own practice, usually, is to highlight passages and write brief comments on a paper copy of an article, take a moment to clear my mind and ask myself what the overall point was and what my overall constructive response is, and then use e-mail to send the author longer and more intelligible versions of those comments. Since I do this quickly after reading the paper (within a couple of days) while my impressions are still fresh in mind, the resulting e-mail messages are limited primarily by how fast I can type. As a result, they can be unusually helpful even though they don't actually take that long to prepare. If necessary I'll also offer to paper-mail the author the marked-up draft for the sake of minor proofreading details that are too much trouble to type in. Notice the fairly complex interactions between paper and electronic forms of communication. You may find different practices more convenient; the point is to be aware that you have a choice. I even know people who tape-record their comments on a paper while they're reading it and then send the author the tape. Keep your real goals in mind and be creative.
- (6) Follow up. This is the one area where e-mail makes a qualitative difference. Once you've established a professional relationship with someone, e-mail provides a convenient way to maintain a steady, low-key background of useful two-way interactions. You might wish to forward things to people (abstracts, interesting messages, conference announcements, press releases, book reviews, whatever) depending on their interests. Don't overdo it and pay attention to whether the gesture is being reciprocated. After a (long) while you might consider building an electronic mailing list of people who share your interests and would like to get interesting stuff forwarded to them routinely -- including, of course, your own abstracts and shorter papers. Never add anybody to such a list (or any list) without asking them, and never pressure them or make a big deal out of it. E-mail is also obviously useful for a wide variety of other purposes, for example scheduling and organizing professional events. Make sure that some purpose is actually being served; don't engage in e-mail correspondence simply for

the sake of it. And don't do any of this stuff with someone unless you've gone through the previous five steps and established a real, functioning relationship with them. Finally, double-check that you're keeping track of the difference between a professional relationship and a personal relationship. A good test is, would I call this person up on a Friday night and suggest going to a movie? Even then, give any such transition in the relationship a little time to sink in before you start to rely on it.

Let me conclude with some comments about community-building. Electronic networks provide a number of technical means for assembling groups of people into semi-structured forms of communication. Most of them are modeled on paper-mail mailing lists, though many people have been experimenting with other mechanisms. And no doubt some of these mechanisms will prove useful. My point here, though, is to ensure that you view community-building in a broad context. A community is made of people, not computers. It is tempting to simply announce a new mailing list, gather lots of names, and hope that something good happens. I've done this myself. Unfortunately, it rarely works very well. Even when you do start feeling good about some of the interactions you've had on the net, human possibility really does run deeper than abstract network-interaction is likely to afford any time soon. In short, I see no substitute for the hard human work of building community one person at a time, on the basis of openly explored shared interests, through interactions in a variety of media. Communities built in this fashion hold together because they are fastened with the real glue of human relationship, not just the technical glue of codes and files. This is not to say that electronic media are useless. Quite the contrary, I've just explained several ways in which e-mail can accelerate the already existing process of building professional relationships. And just as relationships are conducted through a variety of media, so are communities. A community has to meet in person (preferably somewhere nice), eat and drink as a group (preferably in a memorable way), discuss various formulations of the shared vision that brings them together (without trying to force a false consensus), engage in concrete collective projects (editing books, running workshops), and so forth, and suitably constructed electronic media will often have a useful role to play in these activities. This is not the place to explore this process in detail, but I hope the first principles are clear:

- * Cultivate an understanding of the social logic of community-building.
- * Use electronic media as part of a larger ecology of communication.
- * Try out new mechanisms, but don't make them substitute for human contact.
- * Consciously improve and evolve existing ways of doing things.
- * Let it take time.

You may be overwhelmed at this point by the degree of structure I seem to be placing on your electronic interactions. But while these guidelines are not set in stone, neither are they arbitrary. They are simply an application to electronic communications of the larger, preexisting social logic of professional communities. I've restricted my attention to one kind of

community, namely research communities based on publication. But every other kind of community has its own social logic and therefore its own particular structured ways of using various media. If you don't like the structures you encounter, please go right ahead and start changing them -just make sure you're changing things down here on earth, amidst your actual relationships with actual people, and not in an abstract technological head-space. If the structures do sometimes seem arbitrary, that's because we're all accustomed to thinking of electronic media as a world unto themselves, sealed off from the ordinary corporeal world. Where did we get this idea of cyber-reality as a wholly separate sphere? We got it from the fantasy system that underlies a great deal of technical work: the masculine transcendentalism that identifies technology -- and especially computers -with a millenial escape from imperfections and bodies and the accidents of culture and history. By learning to use electronic media wisely, we do more than help our own careers -- we also contribute to a vision of community that acknowledges human life as it actually is.

Appendix: Some references on networking. First, here are some general guides to professional networking, without any special reference to electronic mail:

Donna Fisher and Sandy Vilas, Power Networking, Austin: Mountain Harbour, 1992. This is the best all-around book on the subject. It abstracts a long list of guidelines that apply just about as much to research people as to the corporate people who are their main audience.

Susan Roane, The Secrets of Savvy Networking, New York: Warner, 1993. An adequate book on networking, less sophisticated and narrower in application than Fisher and Vilas' book but much more widely available.

Tom Jackson, Guerrilla Tactics in the New Job Market, second edition, New York: Bantam, 1991. A truly inspired book on the networking that's involved in finding a job through the "hidden job market" of hiring referrals.

Joan M. Brandon, ed, Networking: A Trainer's Manual, Amherst: Community Education Resource Center (225 Furcolo Hall, School of Education, University of Massachusetts, Amherst MA 01003), 1982. Developed for people in community education, this is the most conceptually sophisticated book on the list. Last I heard, it was available by mail-order from the above address for \$9.25.

The modern project of articulating guidelines for networking originates (more or less) with feminist authors of the 1980's. Their books still hold some interest:

Carol Kleiman, Women's Networks: The Complete Guide to Getting a Better Job, Advancing Your Career, and Feeling Great as a Woman Through Networking, New York: Lippincott and Crowell, 1980. Aimed at women professionals and executives who wish to set up relatively formal networking organizations.

Ann Boe and Betty B. Youngs, Is Your "Net" Working?: A Complete Guide to Building Contacts and Career Visibility, New York: Wiley, 1989. A later book in the same spirit, more ambitious but less successful than the others,

based on (fictional?) stories about mistakes people make in their networking activities.

Betty Lehan Harragan, Games Mother Never Taught You: Corporate Gamesmanship for Women, New York: Rawson, 1977. Although not centrally concerned with networking, I mention this book because of its cultural influence as the first hard-hitting how-the-world-really-works book for professional women. Its ideology, which has shaped many feminist discussions of networking since then, reflects both the strengths and weaknesses of the feminism of that era. One of the weaknesses is its inattention to social class; it explains that men learn how the world work through playing football, even though this would predict that working-class men would be as successful in business as their wealthier brothers.

And here are a few references for business-oriented literature on contemporary patterns of networking:

Lee Sproull and Sara Kiesler, Connections: New Ways of Working in the Networked Organization, Cambridge: MIT Press, 1991. A general study of organizational uses of electronic mail.

Bernard Michael Gilroy, Networking in Multinational Enterprises: The Importance of Strategic Alliances, Columbia: University of South Carolina Press, 1993. The economics behind ongoing changes in the workings of global companies, in which the boundaries of the enterprise are less clear and employees' own networks have increasing economic consequences.

Howard E. Aldrich and Mary Ann von Glinow, Personal networks and infrastructure development, in David V. Gibson, George Kozmetsky, and Raymond W. Smilor, eds, The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks, Lanham, MD: Rowman and Littlefield, 1992. Approaches to rationalizing and managing the networking process through social psychology, network mapping, and systematic development of networks.

Acknowledgements. This essay has been improved by comments from Robert Barger, Harry Collins, Paul Dourish, Rebecca Henderson, Marty Hiller, Yvonne Rogers, Susan Sterne, Jozsef Toth, and Jeremy Wertheimer.

Advertisement. Consider subscribing to the Red Rock Eater News Service, an automated mailing list to which I send whatever strikes me as interesting on my trips around the Internet, as well as further articles like this one. To subscribe, send a message to rre-request@weber.ucsd.edu with the subject line "subscribe firstname lastname" (without the quotes). An example would be "subscribe Jane Doe". For more information, send a message to that same address with the subject line "help".

[The E-Mail of the species is more deadly than the Mail. PGN]



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 13

Thursday 14 October 1993

Contents

Software safety on UK national news

Jonathan Bowen

Warning labels on medication

Bob Campbell

Corrigenda: RISKs of trusting e-mail

Theodore M.P. Lee

Risk of brain-dead mailers...

Graham Toal

Draft Italian Antivirus Law

Luca Parisi

Collins autopilots have a mind of their own

Peter B Ladkin

Lufthansa in Warsaw

Peter B Ladkin

Lest you think that all is rotten in the state of aviation this week

PBL

Dr. Strangelove (was Re: auto-response missile system)

Barry Brumitt

Re: ITAR issues in PGP & Moby Crypto subpoenas

Dorothy Denning

Privacy

Phil Agre

Mathematics of Markets

Mark Brader

Book on Risk Perception

Anthony E. Siegman

Re: CFP "Ethics" Workshop Cuba Feb.1994

a.e.mossberg

Re: Cancer Treatment Blunder

Sean Matthews

Bear Giles

New Journal: High Integrity Systems

Russ Abbott

Info on RISKS (comp.risks)

Software safety on UK national news

<Jonathan.Bowen@prg.ox.ac.uk>
Thu, 14 Oct 93 10:50:18 BST

The Wednesday 13th October 9 o'clock evening news on BBC1 TV in the UK featured a new report from the UK HSE (Health and Safety Executive) which includes concerns about the software in the new Sizewell B nuclear plant in the UK. Darlington in Canada was also mentioned and Prof. David Parnas made a brief appearance voicing his concerns on the issues in this area. The report says the "software is of a high quality" but expresses doubts that the safety levels claimed can be achieved. Does any RISKS reader have a full reference for the report?

Jonathan Bowen, Oxford University

Warning labels on medication

Bob Campbell <campbelr@hpcss01.cup.hp.com> Tue, 12 Oct 93 23:18:30 -0700

A thread in sci.med.pharmacy was discussing warning labels on medication. It seems that the computer systems that most pharmacies use now print the labels that the system thinks should be placed on each prescription. These labels are the warnings such as "May cause drowsiness".

The risk is obvious. But a new California law may make matters worse. The high cost and low availability of pharmacists has led to the creation of Pharmacy Technicians. These positions require, at most, a junior college certificate. These technicians may fill prescriptions under a pharmacist's supervision, but may not dispense medication.

Pharmacists I know will override the computer and put the stickers that they know to be correct on. The techs will probably not know, and the quality of the supervision will not replace the quality of a trained pharmacist.

Also, how many hackers could pass up the opportunity to spread around a few erroneous "For rectal use only" stickers on certain managers prescriptions :-)

Bob Campbell campbelr@cup.hp.com

Corrigenda: RISKs of trusting e-mail

Theodore M.P. Lee <tmplee@tis.com> Mon, 11 Oct 1993 23:40:53 -0600

It takes a tough hide to be a reporter. My note in <u>RISKS-15.06</u> on the RISKs of trusting e-mail generated a modest flurry of responses pointing out some errors and asking for some clarifications. Since all who sent me notes could

just as well have sent them directly to RISKs, I am assuming that even though they want parts of the record set straight they don't want to do so publicly. Although I know my "sources" on the scene were convinced of the accuracy of what they told me, by the time the information passed into their hands it seems that some of it was slightly garbled, although not badly enough to weaken the essential point of the whole incident.

(Not to detract from the seriousness of the situation, I do have to note that none of the email pointing the following out was digitally signed or authenticated.)

- 1. The secretaries of the principal figures involved in the resignation message did not take the *contents* of the message seriously. However, they took its existence seriously, believing it indicated there had been a serious compromise of the security of their office information systems. The incident itself has "undermined the confidence" of the clients of the University's computer systems. (This is new information which I think makes the incident actually of more interest than the original version.)
- 2. The FBI was not called in and the students (three, not five) were not expelled, but reprimanded and (temporarily, according to another source) denied their e-mail privileges. I suspect here my sources were telling me actions that were being contemplated but upon which a final decision had not yet been made.
- 3. It was not really fair to mention the name of the mail client the students used, since that is irrelevant and not the source of the problem: it is the SMTP protocol and the inherent insecurity of the internet that give the opportunity. One doesn't even need to have an e-mail program to forge an e-mail message: telnet works just fine.
- 4. "PEM" stands for "Privacy Enhanced Mail." See internet RFC's 1421, 1422, 1423 and 1424; implementations for a variety of platforms are available. (temptation to insert commercial here resisted.) PEM provides digital signatures, authentication, and encryption.
- 5. "6,000" of course is not the size of the student population at the U of W, but some could have read my note that way. The number of students, all of whom are eligible for an e-mail account, is about 41,000. "6,000" (the number now is actually closer to 7,000) is the number who have signed up for it so far.

Ted Lee, Trusted Information Systems, Inc., PO Box 1718, Minnetonka, MN 55345 612-934-5424 tmplee@tis.com

Risk of brain-dead mailers...

Graham Toal <gtoal@gtoal.com> Fri, 24 Sep 1993 16:38:11 +0000

For *years*, attmail.com has been running a brain-dead X400 mailer (Are there any other kinds of X400 mailer?) that regularly causes a flood of bounce

messages whenever anyone posts to a newsgroup that is gatewayed to a user on their system. The name of Brad Hicks (poor guy) must be known by just about every poster to comp.org.eff.talk, for instance.

Well, this is merely annoying, but not _risky_... so where does the risk come in? Look at this (short) extract from the (long) bounce message:

 $From: mc/S=E-Mail_Services_Administrator/OU=0205216@mhs.attmail.com$

Date: 25 Sep 93 01:19:19 GMT

Proper name:

First name : Brad Last name : Hicks

X.400 O/R name attributes:

Country: US

ADMD : ATTMAIL
PRMD : MASTERCARD
Org unit 1 : 0205925

Postal address:

Street: nnnnn Lackland Road Town: St. Louis, MO nnnnn

Fax: 314-275-nnnn

Isn't this fascinating? We now know Brad's employer, home address, home fax number, and some magic number that would no doubt be of use to someone up to no good if they knew what it meant :-) Anyone want to bet this info came from internal attmail.com information and not from something public like a finger file?

Maybe Brad should have a word with attmail.com ... (or change to almost any other non-X400 system in the world that doesn't seem to have these repeated problems...)

Graham

PS I'd have mailed this to Brad but I've *never* in my life managed to mail to anyone with an X400 address. But hey - this *is* the standard that the British Government tells all its organisations to adhere to. Jeez.

[Brad kept trying to get added to the RISKS list, but I could never get mail through to him reliably. The other annoying thing about ATTMAIL is that I had to create a macro with a single mailing for each recipient; it would not accept multiple addressees. I don't know if that is still the case. (This item certainly seems timely after Phil Agre's contribution in RISKS-15.12.) PGN]

Draft Italian Antivirus Law

Luca Parisi <MC1980@mclink.it> Wed, 13 Oct 93 23:48:06 CET

Prompted by the message by Mr. Brunnstein in <u>RISKS-15.11</u>, I thought RISKS readers might find it interesting to know that a "Computer Crime" act is

currently under review by the Italian Parliament (to the best of my knowledge, one of its two branches has approved it).

I have enclosed a tentative translation as well as the original text of the article related to "malicious programs". The whole act also addresses other issues such as unauthorized entry or possession of access codes, etc.

A bit of personal comment about the wording of the article: while the Swiss text focuses on the concept of (lack of) "authorization" in order to define the illegal behaviour of both people and programs, there is no such "keyword" in the Italian proposal. Moreover, the provision against "programs ... having the effect of ... damaging a computer or ... the programs or data contained in ... it" is even more RISKy. It seems to me that, besides viruses, most of the bugs usually found in SW could fall under this article, since the unintentionality is not regarded as a matter of exclusion from the punishment.

Having followed the VIRUS-L forum for a while, I am perfectly aware that it is almost impossible to draw a satisfactory border between malicious programs and legitimate ones, but I feel that this text misses the point by more than a bit. Comments welcome.

Luca Parisi.

- --Proposed Translation--
- --Disclaimer: Please note that I'm not a lawyer, so people in the legal field might find it inaccurate; feel free to correct it if needed--

Article 4 of the [Proposed] computer crime act:

[material deleted]

"Article 615-quinquies of the Penal Code (Spreading of programs aimed at damaging or interrupting a computer system).

Anyone who spreads, transmits or delivers a computer program, whether written by himself or by someone else, aimed at or having the effect of damaging a computer or telecommunication system, the programs or data contained in or pertaining to it, or interrupting in full or in part or disrupting its operation is punished with the imprisonment for a term of up to two years or a fine of up to It. L. 20,000,000."

- --Original Text--
- --Excerpt from: Camera dei Deputati Disegno di Legge presentato dal Ministro di Grazia e Giustizia (Conso), recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in materia di criminalita' informatica." N. 2773--

Art. 4 [omissis]

"Art. 615-quinquies. - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico). - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o

ad essi pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, e' punito con la reclusione sino a due anni e con la multa sino a lire venti milioni."

Collins autopilots have a mind of their own

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
13 Oct 93 17:26:13 BST (Wed)

Flight International, 13-19 October 1993, contains the following report:

(Guy Norris in LA): A succession of autopilot anomalies in Boeing 757s and 767s has prompted calls from the US National Transportation Safety Board (NTSB) for corrective actions and revised operating procedures.

In a 15 June incident at Frankfurt, Germany, a United Airlines 767-322-ER ran off the right side of the runway at 130kt (240 km/h) during a landing roll-out, when the rudder made an uncommanded movement 16deg-17deg to the right, with the nosewheel about to touch down.

The crew managed to deflect the rudder and curve left, but missed another aircraft by less than 90m (300ft) as it [sic] returned to the runway. "Once on the runway, the pilot reported that he regained `soft normal' rudder pedals after pressing the autopilot disconnect button twice," says the NTSB.

Boeing says that it is still mystified, but adds that tests have found "...no evidence at all to link the autopilot with the rudder anomaly". It adds: "We are taking it seriously and tests are continuing."

All 757 and 767 operators will be notified of updated test results by 20 October.

Boeing admits that it did discover a fault which had caused anomalous displays on the mode-control panel (MCP), but it sees no connection with the rudder event.

The NTSB recommends that Boeing and autopilot supplier Rockwell-Collins address `...the uncommanded movements and errors seen in Boeing 757/767 MCP displays and switching functions" [punctuation sic].

It wants the US Federal Aviation Administration to issue an airworthiness directive implementing the changes and to check on the Boeing 747-400 and Fokker 100, which have similar autopilots.

It also recommends that the FAA require Boeing to "...issue a temporary Airplane Flight Manual Supplement to ensure that pilots are aware that autopilots have engaged, disengaged and changed modes and MCP display window setting without pilot input".

[End report]

It seems that the NTSB and Boeing are disagreeing on whether there have been incidents of uncommanded autopilot control inputs. The Independent (newspaper) reported the NTSB comments on the front page on October 12th. Their report is less accurate (even misleading) in a number of respects than Flight's, but there are some more numbers:

(from The Independent, p1, Oct 12th 1993):

[....] On checking United's records, the US National Transportation Safety

Board found that there had been 29 instances - all but one since 1985 - in which autopilots on 757s and 767s had behaved unpredictably [meaning what? `uncommanded control input'? pbl]. Boeing says that most of these incidents involved faulty readings during flight which were corrected by the crew.

[....] Investigators are mystified by the faults since the autopilot is a triple system, including two back-ups to ensure there is no failure. [they've obviously been reading up on Byzantine disagreement - pbl]

[End quotes]

Peter Ladkin

✓ Lufthansa in Warsaw (no, this isn't the new Philip Glass opera)

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
13 Oct 93 20:19:37 BST (Wed)

Flight International, 13-19 October 1993, reports (no byline):

A delay between pilot selection and physical actuation of spoilers and reverse thrust has emerged as a suspected key factor in the runway overrun on 14 September of the Lufthansa Airbus A320 at Warsaw Airport, in Poland. [...] The pilots were also not kept informed by the Warsaw tower of surface-wind changes. After touching down 700m (2,300ft) from the [Runway 11] threshold [.....] the pilots selected spoilers and reverse thrust, but there was a delay of 9s before they deployed, according to the sources.

Actuation of the spoilers may have been prevented by a safety system designed to prevent their deployment in flight: automatic deployment depends on the wheels spinning up at touchdown to a speed greater than 72kt (135 km/h), but aquaplaning may have prevented wheel spin-up.

Reverse-thrust actuation may have been prevented by another safety system designed to stop the operation of reverse thrust in flight [pursuant to the Lauda Air accident conclusions]. An undercarriage microswitch isolates the reverse-thrust actuators until the aircraft's weight is on the wheels.

If the spoilers did not deploy, hardly any of the aircraft's weight would have been on the wheels, a factor accentuated by the pilot's decision to add 20kt to the aircraft's indicated airspeed [they mean: to add 20kt to the indicated airspeed designated for an approach under normal conditions, and use this as the target airspeed for the approach] because of possible windshear on approach [this is a normal procedure, but I rely on other sources for the 20kt figure]. The extra speed would have provided additional lift, reducing still further the weight on the wheels.

Another vital point is that the Warsaw tower controller does not have a surface-wind read-out, but relies on a voice update every 3min from the meteorological department [!!!!!]. As a result, the crew was given a reported surface wind of 160deg/10kt when it [sic] was a tailwind of 280deg/20kt at touchdown [they landed on Rwy 11, which has an orientation of between 105deg and 114deg].

The Polish accident-investigation bureau says that it expects this week to issue its first statement on the accident.

[End quote]

This seems to me like a failure of requirements specification. Weight-on-wheels, and wheels-spinning, are both secondary criteria for landing, as demonstrated categorically by the anticipated report. May I suggest a primary criterion?: Close proximity to ground, in a landing configuration, with spoilers and reverse-thrust selected by the pilot.

Whether Airbus is able to maintain its reputed stance that the software is 100% correct may depend on whether they consider requirements specification to be part of `software'.

Peter Ladkin

Lest you think that all is rotten in the state of aviation this week

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
13 Oct 93 20:34:22 BST (Wed)

Flight International, 13-19 October, also reported that the B747-400 that landed in the drink in Tahiti *did not* yield "evidence of a fault in the full-authority digital engine-control systems on the General Electric CF6-80C2 [engines]." There's a lovely picture of the aluminum overcast slaking its thirst in the ocean.

Peter Ladkin

[Pun-itive measures are needed for pbl. Maybe someone has to pound "stirling" into the briny. Den-mark it well, Laertkin! Drinking in Tahiti in this manner is NOT a good idea. PGN]

Dr. Strangelove (was Re: auto-response missile system)

Barry Brumitt <belboz@frc2.frc.ri.cmu.edu> Wed, 13 Oct 93 17:24:46 EDT

Brian Kenney writes:

The system would be triggered if automatic sensors - which Blair said may be subject to error - detected a disruption of key military communication links, as well as seismic disturbances, and flashes caused by nuclear detonations inside Russia.

I think it prudent at this point to remind everyone of the classic "RISKS" movie "Dr. Strangelove -- or How I Learned to Stop Worrying and Love the Bomb." (Stanley Kubrick directs, Peter Sellers plays 3 roles.)

Roughly, a crazed US Commander sends his wing of B-52's to bomb Russia, and then it is revealed the USSR has something like what Brian discusses above (The Doomsday Device, I beleive). They try to recall the planes, but one has a damaged encryption unit, so recall orders cannot easily be given.

A simple RISKY mistake (a system designed without proper safeguards) and annihilation is made imminent. It sounds rather like a scenario which may play itself out, should this device actually exist -- which, terrifyingly, it now may!

This movie is a *must-see*, particularly in this RISKS context.

[Old stuff, but this item is included for our younger readers. PGN]

Re: ITAR issues in PGP & Moby Crypto subpoenas

Dorothy Denning <denning@cs.cosc.georgetown.edu> Wed, 13 Oct 1993 17:51:50 -0400 (EDT)

In RISKS 15.11, Larry Detweiler wrote the following about import of crypto:

No defense article may be imported into the United States unless (a) it was previously exported temporarily under a license issued by the Office of Munitions Control; or (b) it constitutes a temporary import/in-transit shipment licensed under Section 123.3; or (c) its import is authorized by the Department of the Treasury (see 27 CFR parts 47, 178, and 179)."

According to the ITAR, "Permanent imports of defense articles into the United States are regulated by the Department of the Treasury." My understanding is that Category XIII of the munitions list, which includes encryption technology, has been removed from the munitions import list. Thus, as near as I know, there are no controls on permanent imports of encryption technology.

Dorothy Denning

privacy

Phil Agre <pagre@weber.ucsd.edu> Thu, 14 Oct 1993 12:35:23 -0700

I highly recommend a paper by Victoria Bellotti and Abigail Sellen of Xerox EuroPARC entitled "Design for privacy in ubiquitous computing environments". Bellotti and Sellen demonstrate a structured method for articulating a wide range of privacy problems that can arise with a potentially invasive computer-based technology. The method is not nearly complete, since it does not really address the larger institutional context of such systems, but it is valuable nonetheless. It has been published as part of the ECSCW '93 Proceedings:

Proceedings of the Third European Conference on Computer-Supported Cooperative Work - ECSCW'93. G. Michelis, C. Simone & K. Schmidt (eds.), Kluwer Academic Publishers, Dordrecht, The Netherlands pp 77-92.

It is also available (or at least used to be) as Xerox Cambridge EuroPARC Technical Report EPC-93-103, 1993.

Phil Agre, UCSD

Mathematics of Markets

<msb@sq.com> Thu, 14 Oct 1993 15:57:53 -0400

The October 9 issue of the weekly magazine The Economist contains an extended article of about 20 pages on the topic of "New Frontiers of Finance: The Mathematics of Markets", or in other words, about what computers can and can't do in terms of predicting the behavior of stocks and currencies. While I'm not an expert in that field, the article appeared to me to be very well reasoned and well balanced, and I certainly recommend it.

If you read this too late to buy the issue at a newsstand, you can also mail-order this article alone from The Economist Newspaper Group, Inc., Reprints Dept., 111 W. 57th St., New York NY 10019. The price this way is \$3.50 US (plus tax in CA/DC/IL/MA/NJ/NY/VA/Canada), the same as the cover price of the issue.

Mark Brader, Toronto utzoo!sq!msb, msb@sq.com

Book on Risk Perception

"Anthony E. Siegman" <siegman@sierra.stanford.edu> Tue, 12 Oct 93 14:32:32 PDT

>From the October 1993 issue of the Bulletin of the American Academy of Arts and Sciences:

The University of Michigan Press has released _Risk_ (paperback, \$14.95) edited by Edward J. Burger, Jr., of the Georgetown University Medical School and Institute for Health Policy Analysis. This volume of essays (an expanded version of the Fall 1990 issue of _Daedalus_) grew out of an exploration of how Americans think about risk -- especially risk to health -- and how their views shape their personal and political behavior. It touches on such topics as theories of risk perception, the many ways in which public views about risk have colored government activity, the role of the civil justice system in regulating public risk and compensating for its consequences, management of risk in sexually transmitted diseases, the quality of media reports on health risks, and the influences of science and scientists on litigation and public policy.

To order _Risk_, call (313) 764-4394.

★ Re: CFP "Ethics" Workshop Cuba Feb.1994

a.e.mossberg <aem@symbiosis.ahp.com> 9 Oct 1993 10:49:14 -0400

US Citizens who attend this may discover a hidden risk: The US State Dept still has a ban on US citizens entering Cuba without prior approval of the state dept, which is usually granted only to state dept employees, cubans expatriates visiting relatives, and "approved" researchers. Violation of the ban could result in federal prison.

Amazingly, the ban applies solely to this small Caribbean island that is a favored vacation spot for Canadians and Europeans. No such ban exists for countries we actually have military interest in, such as Somalia, Iraq, and Bosnia.

andrew mossberg * network manager * symbiosis corporation * miami florida usa (305) 597-4110 * fax: 597-4002 * editor, south florida environmental reader

★ Re: Cancer Treatment Blunder (Wolff, RISKS-15.09)

Sean Matthews <sean@mpi-sb.mpg.de> Mon, 11 Oct 93 10:13:08 +0100

- > ... That would lead to
- > OVERDOSES being applied at different sites to different patients.

This is not true. Radiation therapy is violent because it has to be. Doctors know that in order to (have the best chance of) curing a patient, they have to do a certain amount of violence: too much violence and the chance that the treatment will kill the patient goes up, but too little violence and the chance that the cancer will kill the patient goes up. Doctors do not do wilful damage to their patients.

Too low a dose is just as bad as too high a dose; dying of cancer is just as unpleasant as dying of radiation burns.

Sean

Re: Cancer Treatment Blunder (Bakin, RISKS-15.08)

Bear Giles <bear@tigger.cs.colorado.edu>
Mon, 11 Oct 1993 11:27:18 -0600

I remember a glowing _Discover_ magazine article describing how perfect the Hubble mirror was.... The Hubble mirror was tested, but as I recall it was *management* which balked at the necessity of building a second test jig because of a few anomalous measurements. (And don't forget they didn't have access to the DoD test equipment!)

Since everyone seems to believe that testing the output of this device is so simple, do you mind telling us how you're going to model the *human* in the calibration? Can you use a side of beef, or would that introduce too many

errors? Would you need to surgically implant sensors into cadavers? Would the fact that they (obviously) don't have circulating blood, aren't breathing, etc., make a difference in your measurements -- a living patient is always moving around, to some extent.

I'm not arguing that testing shouldn't be done. I'm simply pointing out that it involves quite a bit more effort than sticking a radiation meter on the platform and turning on the power.

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

New Journal Call for Papers: High Integrity Systems

Russ Abbott <abbott@aero.org> 14 Oct 1993 14:26:36 GMT

The new Oxford University Press journal "High Integrity Systems" will explore issues related to systems that either require high integrity or exhibit it, or both.

- o Systems may require high integrity because failure leads to critical losses. Typically these are systems that affect human safety, environmental stability, finance, or some aspect of the societal infrastructure.
- o Systems may exhibit high integrity because they have evolved mechanisms to survive the kinds of shocks their environments may offer.

Although redundancy, fault tolerance, and reliability are important properties of many high integrity systems, the journal is not solely about these features. Its focus is broader. Its aim is to provide an interdisciplinary platform for the examination of mechanisms that allow systems to accomplish their objectives in the face of both anticipated and unanticipated obstacles. Strategies used by both computer-based and naturally occurring systems are of interest. Papers focusing on the design, analysis, and explication of such mechanisms and strategies are solicited. Analyses of the social and legal consequences of losses of system integrity are also of interest. Original research, case studies, and tutorial and survey articles are all welcome.

The journal is supported by an international editorial board. All papers are fully refereed. Electronic submission is encouraged. Publication of accepted papers within six months of submission is anticipated.

For author information contact either:

Editor: A. D. McGettrick, University of Strathclyde, Glasgow G1 1XH, UK adm@cs.strath.ac.uk

Associate Editor: R. J. Abbott, California State University, Los Angeles, CA 90032, USA rabbott@calstatela.edu, OR The Aerospace Corporation, PO Box 92957, Los Angeles, Ca 90009, USA abbott@aero.org

Announcements and news items are welcomed by: P. A. Bennett,

Centre for Software Engineering Ltd., Scunthorpe, UK



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 14

Monday 18 October 1993

Contents

Cable company shows unorthodox children's TV

John Gray

Risks of Virtual Reality

John Mainwaring

Re: Wiretap Laws and Procedures

Bob Leigh

Robert Firth

Hubble mirror errata

Henry Spencer

Re: Privacy Risk for Toronto Dominion Bank customers

Dave Parnas

Digital Signatures as ID Numbers

Karl J. Smith

File on Four

Pete Mellor

Australian government to replace DES

Kevin Burfitt

The FAA and HERF

Winn Schwartau

Info on RISKS (comp.risks)

Cable company shows unorthodox children's TV

John Gray <grayjw@cs.aston.ac.uk> Mon, 18 Oct 93 11:11:23 BST

The following events happened about January this year, at our local Cable TV company; I worked for them over the summer vacation and I was told this story by one of the people involved....

Our local cable company makes no local programmes; a voluntary group makes about 40 minutes a month. This is shown every night at 7pm immediately after the close of service of the Children's Channel. Obviously the programs involved are quiet innocuous and suitable for family viewing.

The company also offers a channel called HVC: this shows films which are distributed on tape to the cable operators. The tape format limits each tape to an hour so each film is split over two tapes. HVC's films are low-budget romance and soft porn. Three films of progressively "stronger" content are shown each evening.

Both local programmes and HVC are provided using a bank of tape machines and a "Kavicom" computer system is set up to activate each machine at the right time and send its output to a cable channel.

On this occasion, the employee(X) who normally loaded the machines set up the computer for the evening, but didn't load the tapes because the machines were in use. In fact, one of the machines was unavailable so the tapes were to run in different machines from usual. X would return later and load the tapes.

Slightly later, while X was working elsewhere, employee Y arrives and loads all the tapes (the machines are now available), notices the computer's been set and informs X upon his return that he's set up the system.

At 7.15pm the station's choef engineer is called at home to be told that there's porn on the Children's Channel. About 10 minutes later, someone gets to the [unmanned] station and stops the machines. The error in all this: Y had assumed the setup would be the same as always; X assumed that Y checked the details on the computer. The result: the second tape of the last film (the steamiest) was substituted for the local programmes.

A general note: I've worked with two broadcasters and neither appears to have any real concern about the integrity of their communications links (it is assumed that the service providers for the links will keep them secure). For example, all the TV and radio service for Scotland passes through one site: this makes an obvious weak link (either in terms of vulnerability to takeover or to systems failure). TV and radio signals aren't encrypted (encoded using standard hardware though) for pre-transmission distribution.

Have you ever wondered how much trust you place on what you see on television? Not only that broadcasters will show "appropriate" programs but that the service will provide information when you need it. With larger proportions of the network management being computer-controlled, there seems to me to be ample problems waiting in the wings.

Risks of Virtual Reality

"John (J.G.) Mainwaring" <crm312a@bnr.ca> Mon, 18 Oct 1993 18:06:00 +0000

There was a good deal of discussion on sci.virtual-worlds early in September about potential risks of using HMDs (Head mounted Displays). J. Hill posted a substantial extract from a front page article by Steve Connor and Susan Watts published in the Independent (in London) on Sept. 5. There was lively discussion in several subsequent postings. There are different approaches to HMD design, and approaches that don't use HMDs. Just when we thought we were

learning to deal with the hazards of keyboards and displays, it seems that there are other ways for computers to get us.

Hill's posting and disclaimer follow.

A new toy that allows children to play computer video games in 'virtual reality' could permanently damage their eyesight.

The equipment - a headset which beams stereoscopic images on to both eyes - is already in use in such hi-tech amusement arcades as London's Trocadero. Sega, the Japanese computer games company, intends to launch a home version in the United States later this year, and in Europe next year.

Tests of virtual reality headsets on adults produced visual problems which scientists believe could be far more serious in young children. One fear is that the toys could lead to permanent squints.

Two groups of researchers, one at Edinburgh University and one in the Ministry of Defense, have detected side-effects in adult volunteers who wear the 'head-mounted displays', which produce an illusion of reality by giving all-round, three-dimensional vision of moving objects. Such equipment is already used by the military and by commercial designers who want to see their work in three dimensions.

The Health and Safety Executive has set up an investigation of the headsets because of fears raised by a research team led by John Wann, a lecturer in human perception at Edinburgh. 'Our results suggests it seems particularly unwise to introduce them as a toy for children,' Dr Wann said. 'If they are spending more than a few minutes with these headsets, there are serious considerations for their eyesight.'

Mark Mon-Williams, an optometrist, said that people who used the headsets for 10 minutes showed similar visual disturbances to those who spend eight hours at a computer screen. 'It's amazing what you are asking your eyes to do inside the headset,' he said.

Of 20 young adults who took part in a 10-minutes test, 12 experienced side-effects such as headaches, nausea and blurred vision. Mr Mon-Williams said that a particular concern is that the headset puts a lot of strain on binocular vision, which is fully developed in adults but is more liable to break down under stress in children under 12 years, causing squints.

The Edinburgh findings are supported by researchers at the Army Personnel Research Establishment at Farnborough, Hampshire. In a test, 61 per cent of 150 volunteers reported symptoms such as dizziness, headaches, eyestrain, light-headedness and severe nausea.

Mr Mon-Williams said the main problem stems from the headsets severely straining the eye muscles, leading to slightly cross-eyed vision. A slight misalignment of the two images in each eye produces a visual disparity that the muscles try to correct.

Andrew Wright, software product manager for Sega in Britain, said that the new product would be tested extensively before coming on the market.

Other health problems associated with virtual reality are beginning to emerge: a form of travel sickness is affecting people who spend too long in virtual environments. Symptoms such as nausea and disorientation are brought on by the slight time-lag between people moving their head and the scene they are immersed in 'catching up'."

[I would say that Sega and the rest of the VR games manufacturers have some PR work to do. I will watch the Independent for any responses to this article. J. Hill, unrelated to University of Edinburgh research team cited in the article.]

✓ Wiretap Laws and Procedures (Denning, RISKS-15.10)

Bob Leigh <bobleigh@world.std.com> Fri, 15 Oct 1993 16:32:26 -0400

>Typically, a court order is requested after a lengthy investigation and the >use of a "Dialed Number Recorder" (DNR). The DNR is used to track the >outgoing calls from the suspect's phone in order to demonstrate that the >suspect is communicating with known criminals. [...]

>Electronic surveillance is a tool of last resort and cannot be used if other >methods of investigation could reasonably be used instead. Such normal >investigative methods usually include visual surveillance, interviewing >subjects, the use of informers, telephone record analysis, and DNRs.

This implies that applying a DNR to a suspect's line does _not_ require a court order and is not considered wiretapping. In other words, the list of numbers called by a suspect is not protected as rigorously as the content of those calls. I'd like to hear more about how this data is protected or made available to investigators and others.

I think it would be possible to deduce a great deal about a person's lifestyle and associated from the list of numbers he or she calls. This is the inversion, in a pseudo-mathematical sense, of the database that could be created by a Caller ID subscriber. Surely possession of this information should ordinarily be limited to the caller and the telephone carrier?

★ Re: Wiretapping (Denning, RISKs-15.10)

<firth@SEI.CMU.EDU>
Fri, 15 Oct 93 11:55:10 -0400

Dr. Denning's long article on wiretapping was most informative. This section in particular caught my attention:

(4) major offenses involved (634 narcotics, 90 racketeering, 66 gambling, 35 homicide/ assault, 16 larceny/theft, 9 kidnapping, 8 bribery, 7 loansharking/usury/extortion, 54 other)

If we exclude "other", and also "racketeering", which is a catch-all term like "offensive to Allah and corrupt of the earth", then, of the 775 major offenses involved, no less than 700, or 90%, involve victimless crimes, ie actions involving only consenting adults in free-market transactions.

In other words, these wiretapping capabilities are not being used against real crimes, but against actions that are defined as criminal for no better reason than that Leviathan has a boot with which to stamp, and we have faces to be stamped on.

The risk, I guess, is rather an old one: too many of us are in danger of forgetting that liberty is indivisible.

<henry@zoo.toronto.edu>
Fri, 15 Oct 93 12:41:38 EDT

>I remember a glowing _Discover_ magazine article describing how perfect the >Hubble mirror was...

The Hubble mirror actually was quite strikingly precise; it matched the (incorrect) test rig -- the specification, so to speak -- with unprecedented exactness.

- >The Hubble mirror was tested, but as I recall it was
- >*management* which balked at the necessity of building a second test jig >because of a few anomalous measurements...

Not quite correct. There were three test rigs built for that mirror, and two of them reported the error. It happened that the third was considered the most accurate, so management -- under considerable pressure -- ignored the results from the other two.

There was never any serious consideration of building the sort of test setup that would have been needed for an "end-to-end" test. Quite apart from the cost, and the perceived unlikelihood of finding anything -- this really was a one-in-a-million mistake -- it would have added substantial risks of contaminating the mirror surface.

Incidentally, something to think about, with the repair mission imminent... Obviously, one crucial input to the manufacturing of the corrective mirrors was the exact error in the primary mirror. This could be measured in two ways: by examining the test rigs and results used to make the mirror, and by examining the images from the telescope (with its focusing adjustment in various positions). The two methods do not quite agree. The discrepancy is quite small, but it is larger than the known errors of the two methods (that is, the error bars don't overlap). By itself, it's probably not a problem -- the positions of the corrective mirrors can be adjusted from the ground to deal with minor errors -- but it does suggest that the situation may not be completely understood.

Henry Spencer at U of Toronto Zoology henry@zoo.toronto.edu utzoo!henry

Re: Privacy Risk for Toronto Dominion Bank customers

Dave Parnas <parnas@triose.eng.mcmaster.ca>
Sun, 17 Oct 93 17:27:36 EDT

This months "Bulletin" for Toronto Dominion Visa customers announced the availability of an automated Voice Response System. It makes lots of information, including balance, and the last five payments, available to anyone who knows the card number and 3 digits from the customer's postal code. The card number is given out with every purchase, the postal code is easily obtained from the address available in every telephone book. In other words, anyone can get information about your purchases.

I first became aware of this before I saw any announcement becaused I phoned to make an inquiry. Shocked at this exposure I asked if I could pick a PIN number different from my postal code. I was told that this was not possible with their computers! I then demanded that I be taken off the system and, after talking to 3 levels of employees, this was done.

However, until today's announcement, most customers were not available of the exposure.

Offering the user the choice of a PIN seems the least that they can do, but they won't do it.

Prof. David Lorge Parnas, Dept. of Electrical and Computer Engineering, McMaster Univ., Hamilton, Ontario Canada L8S 4K1 905 525 9140 Ext. 7353

Digital Signatures as ID Numbers

Karl J. Smith <sparcom!karl@uu.psi.com> Sat, 16 Oct 1993 12:58:59 -0800

It looks as though the concept of signing things with digital signatures is beginning to take off, and will surely become more commonplace. This is good, because we don't have to worry quite so much about forged email, etc. A few years from now, when we start using electronic means to order things from businesses, whether it's via email, or through our amazing new "Mall in a Box" piped to us through fiber lines to our TV, we'll also use digital signatures. Nobody will be able to order something posing as us, and credit card fraud should be greatly reduced, since all orders will be digitally signed. This is good, right?

Well, now the businesses have our number. Our public key identifies us, uniquely. Nobody else will have the same public key. This means that businesses no longer have to try to track us down via our SSN or Driver's license number - they've got a much better number to use to refer to us in their database - our signature. We've given it to them voluntarily. That's not so good. Cross-referencing a few of these databases will divulge buying habits

and other personaly information that's been mentioned in RISKS before.

-- Karl J. Smith : SW JOAT -- Sparcom Corporation -- Corvallis, OR karl@sparcom.com : Phone (503) 757-8416 -- FAX (503) 753-7821

File on Four

Pete Mellor <pm@csr.city.ac.uk> Mon, 18 Oct 93 08:20:05 BST

Readers of the list who are able to receive BBC Radio 4 may like to know that this week's "File on Four" is devoted to the subject of risks of complex systems and particularly safety-critical software.

The programme goes out on Tuesday 19th Oct. at 19.20 (just after the Archers! :-) and again on Wednesday 20th at 15.00.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V OHB, Tel: +44(0)71-477-8422, JANET: p.mellor@csr.city.ac.uk

Australian government to replace DES

Kevin Burfitt <zaph@torps.apana.org.au> Mon, 18 Oct 1993 17:14:08 +1000

Here is something I found in an Australian computer magazine, which sounded like something for the Risks Forum...

Quoted from "PCWEEK October 20, 1993"

The Australian Government has secretly developed its own data encryption firmware and algorithm, killing its dependence on the US DES (Data Encryption Standard) Algorithm.

Called Seneca, the firmware element was developed as a joint project of the Defence Science and Technology Organisation (DSTO) in Adelaide and the Defense Signals Directorate (DSD) in Canberra.

[...]

"It is a symmetric encryption technology like DES, but can operate at very high speeds" said the source. Seneca's original specifications included a throughput of 2Mbps, but testing had achieved rates of 20Mbps.

Isn't part of the security with DES its slowness, which implies that this new encryption method will be inherently risky because of its speed?

Kevin Burfitt

zaph@torps.apana.org.au (Kevin Burfitt) Compuserve: 100240,2002

Torps Productions: torps.apana.org.au BBS +61-3-818-0986 FidoNet: 3:635/574

The FAA and HERF

"Winn Schwartau" <p00506@psilink.com> Thu, 14 Oct 93 21:32:17 -0500

The FAA Discovers HERF Is John Q. Flyer In Danger?

On a recent series of US Scare plane flights, I noticed a new flight attendant spiel.

"We're descending below 10,000 feet for our approach into (safe major metropolitan airport). Please turn off all laptop computers, CD and cassette players. Thank you for flying US Scare."

In the July 26, 1993 issue of Newsweek, the following appeared.

"On an uneventful flight over the Southern Pacific last February, the 747-400 pilot stared wide-eyed as his navigational displays suddenly flared and crackled. The data made no sense. But a flight attendant was already whisking a passenger's laptop computer up to the flight deck. When the crew turned it on, the navigation displays went crazy. They returned to normal when the crew switched off the laptop. The plane reached its destination safely. Investigating the incident, Boeing engineers bought the same model laptop and tried to replicate the glitch in another 747. They couldn't."

And then, "In a holding pattern 13,000 feet somewhere above the southeastern United States, the pilot saw the guidance computers and controls that maintain the craft's lateral stability shut down. A passenger in Row 1 - directly above the flight computers and near the navigation antennas - was using a radio transmitter and receiver, a flight attendant said. The first officer hurried back and the told the man to shut it off; the systems blinked back on. Five years later, no one can explain how, or even if, the radio zapped the computers."

Welcome to the world of HERF.

HERF is an acronym for High Energy Radio Frequency, and holds potential disaster within its enigmatic description.

Over the last couple of years, Security Insider Report has discussed HERF and its potential for disrupting electronics (June, 1992, October, 1992, November, 1992, January, 1993). Word is getting out.

A fundamental axiom of electronics is at the heart of the phenomena, and needs to be understood to appreciate the potential severity of the problem. An electric current creates a magnetic field, which travels at the speed of light in all directions. This is the principle of radio and TV and cell phones.

If you stick a wire in the air, and connect it a completed circuit, a magnetic

field will induce a current flow. Again, radio and TV. If you modulate the signal with information, then the information can be sent from one place to another almost instantaneously.

On the other hand, we have all heard interference on the radio or a cell phone when passing through a tunnel or on a bridge.

HERF is the magnetic field, intentional or not, that when detected by an electric circuit can disrupt its operation to varying degrees of intensity.

A HERF signal, if properly aimed at an electronic target can so disrupt its operation as to render it useless.

This may well be what's happening to the 747-400's that experience anomalies such as those Newsweek described. You see, the latest generation of planes are known as "fly-by-wire", meaning that the planes functions, from nose to tail are controlled by a maze of computers and 145 miles of wires and cables. Many of these signals are so-called low-level signals, high impedance low voltage signals that are the most susceptible to interference.

Now, a laptop computer or CD player will emit unintentionally, a quantity of radiation by its very nature. Despite the regulations made by the FCC to minimize electromagnetic emissions on consumer equipment, the shielding is far from complete. While the home computer may no longer screw up a TV picture as it did in the days of the TRS-80 and VIC-20, enough signal leakage occurs as to be of concern to the DoD and NSA. That's why they have the Tempest program - to stop all leakage at all costs. That's an intelligence concern, but the principle is the same.

While the FAA and most airlines deny that there are any safety concerns to worry about, malfunctions of avionics systems do bring up serious public safety issues. Since 1990 the FAA has complied almost 100 reports of such occurrences with a six-fold increase this year alone. Why? We suspect, as many do, that fly-by-wire planes are indeed affected by computers and digital music systems.

The number of potential paths that a radiated signal can take include flowing down the metal skin of the airplane, down the conduits of the wiring, directly into low level paths, or bouncing off of metal surfaces directly into antennas. Another possibility is one of resonance; where the radiated signal and the affected circuitry operate at the same frequency, thus increasing the apparent effects. A 10 MHz signal tends to attract and apparently "multiply" the energy of a nearby induced 10MHz signal. It's the nature of the beast.

Another culprit is the FCC testing method for emissions certification of consumer products, especially computers. The tests as run by the manufacturer are idealized, under nearly perfect conditions. But, if you add RAM or a bigger hard disk, or one from another manufacturer, or use a higher speed CPU or add a modem, the rules change, and the emissions characteristics change. The power supply is drained faster, the clock cycles differently, and the location of the added RAM creates new magnetic patterns that might not still meet the barely adequate FCC emissions standards.

Back in the mid 1980's, I worked for computer companies who spared no effort

in minimizing compliance with the FCC. The bare minimum configurations were tested, and often we had to run back and forth to the factory to find the one single, unique computer system that would comply. Manufacturing tolerances and the bottom line took precedence over compliance.

In many cases, the mere addition of 256RAM, bringing the machine up to a fully loaded 640K, would literally increase the emissions by a factor of 10! The FCC be damned. And then the addition of peripherals were even worse. Only those peripherals which actually had a port or a cable were required to have their own FCC compliance, but there's no provision for the synergistic effects of different manufacturer's products working together and still meeting the specifications. It was a total scam by every company I worked for. The edict was clear: Do whatever it takes to pass the test, for every day we're not selling, we're losing money.

Also, some of the approved FCC testing laboratories were less than on the up and up. A typical suite of tests can run from \$2500 to \$25,000 and take 6 weeks or so; a costly death knoll for the competitive computer biz. But a double payment, in cash, often insured that the product was guaranteed to pass in less than a week. Get the point?

Then there's the mice. A mouse - in distinction to a built in track ball within the unit itself - is attached by a wire. Another word for a wire is an antenna, and antennas are meant to amplify signals. In the case of the mouse, the wire is merely meant to carry stepped signals to the CPU; however, the shield or ground signal, especially in a battery driven laptop, is what we call floating; that is, it never really reaches ground to sink into the power company's and Mother Earth's natural ground point.

Instead it floats at some undetermined level above ground, and guess what it does? It radiates! At some undetermined level, depending upon what is stuck inside the machine and by whom.

It's no wonder that the engineers at Boeing and NASA and Apple are having such a time trying to figure out what's happening. The rules are wrong in the first place.

We live in an electromagnetic sewer, and God knows we shouldn't be playing "let's not worry about it" with computers flying planes at 37,000 feet.

The FAA knows better, and I would hazard to guess, wants to do everything within its power to avoid a panic or loss of public faith in the airline industry. That's perhaps why, they have kept it pretty quiet that they are protecting their own airport based facilities against HERF and radiated emission interference.

In a low-profile massive endeavor, the FAA is replacing the glass in its control towers and offices in and around airports.

We have received information from sources close to the FAA that their very concerned about HERF interference problems in air traffic control systems from the high power radar that keeps the airways safe. According to these sources, they are replacing control tower and office glass with shielded glass which

attenuates electromagnetic signals by anywhere from 60-100db depending upon the severity of the problem.

The replacement program is supposed to last for several years, which coincides with the upgrading of the nations control systems - which will obviously be more automated and computer driven than ever.

If the FAA is as aware of the problem and the possibilities as it appears they are, one would hope they would take some stronger proactive measures to protect passengers - even if they're is only a glimmer of a chance that a laptop or a CD player could cause a plane to crash.

It seems entirely reasonable to suggest that the FAA should just go ahead and ban such electronic devices on planes altogether. What's the big deal? Would the traveling Road Warrior care that he would lose 5 hours of productivity on the Red Eye? Probably, but if all airlines stick to a policy (there's that word again . . . funny how it keeps cropping up) especially is mandated by the FAA, everyone would still be playing on a level playing field, and no one would lose business.

On the other hand, if planes are in fact susceptible to low level emissions from computers, is that such a good thing to openly admit? Because, what if you just turn up the volume a few db?

There are plenty of crazies out there; and with terrorist concerns on the rise, who knows what they might pull. Well, here are a couple of possibilities.

Suppose I'm a real crazy bad guy, and I bring a specially modified laptop onto an airplane. The airport security is dismal and you can get just about any electronic device through with no trouble. But this laptop is modified to emit very high levels of radiation; either automatically or upon command. If I'm real nuts, and am totally committed to my cause celebre, I might be willing to bring the plane down with me on board. More than a few people meet that criteria. It might take a little tinkering and get on the right fly-by-wire plane to do it, but with the number of events already on the books, it's doable.

Or, if my survival is important, I might check my luggage through with a HERF device, timed to 'go-off' at some point during the flight. Without me on board, of course. Luggage scanning can't tell the difference between a 'good' electronic device and a 'bad' one. If the FAA has something to worry about in this realm, this certainly qualifies.

Or, let's replace the rocket launcher at the end of the O'Hare runway scenario which was disclosed by the FBI during a CPSR meeting in Washington, D.C. on June 7, 1993, with a powerful HERF Gun. A HERF Gun is an electromagnetic generator which is focused and aimable and frequency specific. Situated in a van, powered by a V-8 and an alternator, the HERF energy, several orders of magnitude louder than that emitted from a laptop, could have a devastating effect on planes taking off and landing.

And acquiring such devices is pretty simple. You can go out and build one - it's an exercise in Electronics 101 - or I can buy one. Where? From the US

government of course. A military surplus high power radar antenna is easily modified for higher signal strength and focussed targeting by someone familiar with electronics.

Cyberspace has indeed come of age, and modern airplanes are as much a part of it as computer networks.

It's just that the FAA doesn't know what to do about it yet.

Let's hope they get up to speed quickly. Very quickly.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 15

Tuesday 19 October 1993

Contents

Confirmed reservation ... for non-existent flight Mathai Joseph

Physical Security of ATM Password Jeff Schultz

Re: RISKs of trusting e-mail Lars-Henrik Eriksson Frederick M Avolio

Re: Porn, Wiretapping, DES, HERF Phil Karn

Re: The FAA and HERF **Ted Wong**

Jack Boatman

Re: Digital Signatures Robert J Woodhead

Re: Risks of Virtual Reality **Robert Carolina**

Re: Wiretap Laws and Procedures

Steve Bellovin Re: Australian government to replace DES

Steve Bellovin Re: Software safety on UK national news

Pete Mellor Re: Libraries and Imagined Communities **Bruce Hamilton**

Re: Separating parts in privileged applications **Bob Frankston**

Tom Thomson Info on RISKS (comp.risks)

Confirmed reservation ... for non-existent flight

Mathai Joseph <mathai@dcs.warwick.ac.uk> Tue, 19 Oct 1993 09:42:15 +0100

One Sunday in August this year I was booked on a scheduled flight from Buffalo to Ithaca. The ticket was issued in the UK and the reservation was confirmed.

It was a little surprising therefore to be told at Buffalo airport that I had been booked on a non-existent flight: there just is no such flight on a Sunday and the printed timetable confirms this.

How was I issued with such a ticket? The airline informs me that "it is rare for a problem of this nature to occur". Apparently, "when your agency made reservations for the two flights in question, our system accepted the reservation as confirmed even though the flights did not operate". They are "unable to determine where an error may have occurred" but "it is generally thought to be due to a software or message switching malfunction".

That it is "rare" does not really help much. Must I (and everyone else travelling by the airline) now check *every* ticket to ensure both that the reservation status is OK and that there is actually such a flight? Or just some tickets? Which ones?

(For information, this is a large international airline, not a small operator.)

Mathai Joseph

Department of Computer Science, University of Warwick, Coventry CV4 7AL +44 (203) 523987 mathai@dcs.warwick.ac.uk

Physical Security of ATM Password

Jeff Schultz <jws@cs.mu.oz.au> Tue, 19 Oct 93 11:30:43 +1200

>From The Age, Melbourne, 18 October, p. 2:

I'm not happy, said the bloke on the phone to his bank's head office. "What did you have to go and paint it for?"

. . . "My local branch . . . you've just painted the outside of it."

"Um," said the nonplussed executive at the other end,

"You're missing the point. I'd scratched my PIN number into the paint work. Now you've covered it over and I can't use my bloody card!"

A new meaning for "bricks and mortar security."

Jeff Schultz (jws@cs.mu.oz.au)

★ Re: Corrigenda: RISKs of trusting e-mail (Lee, RISKS-15.13)

Lars-Henrik Eriksson < lhe@hume.Informatik.Uni-Tuebingen.De> Fri, 15 Oct 93 10:27:57 +0100

...The incident itself has "undermined the confidence" of the clients of the University's computer systems.

Given the poor security of the e-mail system, perhaps one could say that the incident has given the clients an appropriate level of confidence for the computer systems involved!

Lars-Henrik Eriksson, Wilhelm-Schickard-Institut, Tuebingen University
On leave from the Swedish Institute of Computer Science until Oct. 20, 1993.

★ Re: Corrigenda: RISKs of trusting e-mail (Lee, RISKS-15.13)

Frederick M Avolio <avolio@TIS.COM> Fri, 15 Oct 93 10:57:54 -0400

The *real* problem is the perceptions casual users of computers and computer networks have. A few, but not all, are:

- If you are reading it on a computer, it must be true (similar to people believing photos, television, newspapers, etc.
- Electronic mail is private and untamperable
- Falsification of e-mail indicates that the security of the system, network, or user account has been compromised.

We know that it is easier to falsify e-mail than p-mail, but not *much* easier. It is very easy in every organization I have been associated with (high school, 2 universities, a no such agency in the government, a large computer firm, and now, TIS) to get official stationery. Now, with PostScript and PCs, it is trvial to create your own stationery.

The wet signature on p-mail sets it apart from most (sans digital signatures with or without certificates) e-mail. But, this is significant, in this instance, only if the recipient recognizes the wet signature.

- > 2. The FBI was not called in and the students (three, not five) were not
- > expelled, but reprimanded and (temporarily, according to another source)
- > denied their e-mail privileges. I suspect here my sources were telling me
- > actions that were being contemplated but upon which a final decision had
- > not yet been made.

What organizations need to do is set policy on such rude behaviour. E.g., a statement indicating that misrepresenting yourself as, or impersonating, someone else -- whether in e-mail, p-mail, or on the telephone -- is against the rules and will result in certain sanctions. Faking p-mail is less common because there are a bunch of steps to go through along the way, allowing multiple decision points for the person's conscience to kick in (getting paper, typing, putting in envelope, sealing, addressing, stamping, taking to

mail drop, and mailing). E-mail is typed up and gone in less than a minute. Most e-mail systems treat that like p-mail dropped into a postal box: from that point on it is the "property" of the recipient.

Fred

Re: Porn, Wiretapping, DES, HERF (RISKS-15.14)

Phil Karn <karn@unix.ka9q.ampr.org> Mon, 18 Oct 93 23:56:28 -0700

Several items in this digest struck my interest.

First was John Gray's comments on "porn" accidentally making it onto a CATV "children's channel".

>Have you ever wondered how much trust you place on what you see on television? >Not only that broadcasters will show "appropriate" programs but that the >service will provide information when you need it.

Very little. And I do not expect this to change. I really do wish the population at large would discover the "end to end principle" for itself. They should stop demanding that the CATV companies, satellite uplinkers, broadcasters, video store owners, the government, i.e., anyone and everyone but themselves, be responsible for controlling what they and their children watch.

I have this product idea should make me millions once I patent and sell it to all those easily offended households: it's call an "off switch".

>From firth@sei.cmu.edu's comment on Denning's wiretap article:
>In other words, these wiretapping capabilities are not being used against real
>crimes, but against actions that are defined as criminal for no better reason
>than that Leviathan has a boot with which to stamp, and we have faces to be
>stamped on.

Bingo! This was one of the things that convinced me that the widespread use of strong cryptography to defeat wiretapping will on balance be a Good Thing. But to be honest, when this happens (and it will, whether the government likes it or not) it will admittedly become more difficult, though not impossible, to prosecute a few crimes that actually ought to *be* crimes. Foremost among them is influence peddling and bribery among government officials.

I had resigned myself to this as an unfortunate consequence of an otherwise positive development. But then it occurred to me: the only reason crimes like influence peddling and bribery are possible is because the public has granted government officials so much trust and power in the first place! Who knows? Perhaps one of the consequences of universal cryptography will be a lessening of the power of centralized government and the delegation of much less personal authority to those within it.

Re Kevin Burfitt's note on a new Australian cipher to replace DES, does anyone know if the algorithm will be publicly available?

|> Isn't part of the security with DES its slowness, which implies that this |> new encryption method will be inherently risky because of its speed ?

Not necessarily. DES was originally designed for hardware implementation, and many of its operations are inherently slow in software. A good example are the initial and final permutations, which consist simply of renumbering the input and output bits. This is trivial in hardware but a real pain in software. Some even suspect that these permutations were added solely to sabotage efficient software implementation, as they contribute nothing to the strength of the algorithm. Certainly not to a brute-force keysearch attack, which can be conducted after the permutations have been "factored out".

A new encryption algorithm designed specifically for efficient software implementation could run much faster than software DES without necessarily being less secure. It would use the native operations and native data sizes found on most modern computers. Examples include IDEA and MD5 (although MD5 is not, strictly speaking, a cipher, it does have a cipher-like structure).

|> Subject: The FAA and HERF

Winn Schwartau's article on "The FAA and HERF" is exactly the kind of article we've been seeing far too many of in the media lately. Not because the subject isn't worth investigating, but because the article is long on scary anecdotes, impressive sounding jargon and calls for action, and short on cold, quantitative information and logical reasoning.

The term "High Energy RF" is something I'd associate with broadcast transmitters, long range radars and microwave ovens, not your average laptop computer. Exactly what constitutes "high energy"? A few orders of magnitude would be good enough.

And there are quite a few radionavigation systems in use by commercial aviation, each with its own uses, strengths and weaknesses, including vulnerability to interference. Which ones are we talking about? Over land, VOR and DME are the most common. And they work by two very different principles on widely separated radio frequencies. DME is inherently much more resistant to interference than VOR. ILS (instrument landing system), is a cousin to VOR. It probably has about the same susceptibility to interference, but in a situation with a much smaller margin for error -- which is why many airlines now ban electronics during landing, even though it may not be strictly necessary. And over the oceans you have Omega, operating at VLF frequencies, usually combined with an Inertial Navigation System (INS). (GPS is not yet permitted as a primary navigation reference, and LORAN-C is common in US private planes and helicopters but rare in commercial aircraft.)

So exactly which system was in use by the 747-400 in question? Chances are it was an INS, found on almost all commercial transoceanic aircraft. And INS's main feature is that it lacks a radio receiver, making it virtually immune to

radio interference! This makes the anecdote just a *little* less credible.

Again, I'm not trying to belittle those concerned about interference to aviation navigation. I myself fly frequently with a laptop. If there really were a hazard, believe me, I'd want to know about it. But what we need are some carefully controlled tests producing reliable, quantitative information. The closest I've seen to this appears in the October 1993 issue of PC Computing magazine. They actually measured the RF emissions from a variety of personal electronic devices, including cellular phones, AM/FM broadcast radios, walkmans, laptop computers, CD players and handheld games. Their conclusion:

"...it was highly unlikely for laptops and most PEDs [portable electronic devices] to cause navigational interference. Of the devices tested, nearly half produced signals so weak they couldn't be measured above the baseline noise present on all radio frequencies... In general, we were unable to produce any real VOR interference except when we used FM receivers and cellular phones, and when we placed other devices unrealistically close -- within 6 to 12 inches of the VOR receiver antenna."

Phil

★ Re: The FAA and HERF (Schwartau, RISKS-15.14)

Ted Wong <tmw5@cornell.edu> Tue, 19 Oct 1993 00:50:15

>"We're descending below 10,000 feet for our approach into (safe major >metropolitan airport). Please turn off all laptop computers, CD and cassette >players. Thank you for flying US Scare."

A recent issue of PC Magazine conducted a series of tests using an HERF detector to determine the amount of leakage generated by portable computing equipment. They found that common equipment did NOT generate HERF interference above the background noise level. In other words, apart from widespread anecdotes, there is yet no evidence to back up claims that portable computers are responsible for interfering with in-flight equipment. I accept that the author's experience with corrupt FCC certification labs means that some very badly made portables could be exceptions.

However, PC Magazine did find that most common non-computing devices, such as Discmans or Walkmans, DID cause measurable levels of HERF interference. It is conceivable that if such a device is used close to a control board, interference will occur.

[Incident involving possible HERF interference due to a laptop.] >Investigating the incident, Boeing engineers bought the same model >laptop and tried to replicate the glitch in another 747. They couldn't."

This demonstrates the point of the first paragraph. All that is available are anecdotes, which show only a weak cause/effect link, and which in many cases aren't reproducible.

>There are plenty of crazies out there; and with terrorist concerns on the >rise, who knows what they might pull. Well, here are a couple of >possibilities.

>Suppose I'm a real crazy bad guy, and I bring a specially modified laptop onto
>an airplane. The airport security is dismal and you can get just about any
>electronic device through with no trouble. But this laptop is modified to
>emit very high levels of radiation; either automatically or upon command. If
>I'm real nuts, and am totally committed to my cause celebre, I might be
>willing to bring the plane down with me on board. More than a few people meet
>that criteria. It might take a little tinkering and get on the right
>fly-by-wire plane to do it, but with the number of events already on the
>books, it's doable.

>Or, if my survival is important, I might check my luggage through with a HERF >device, timed to 'go-off' at some point during the flight. Without me on >board, of course. Luggage scanning can't tell the difference between a 'good' >electronic device and a 'bad' one. If the FAA has something to worry about in >this realm, this certainly qualifies.

While the possibility of HERF interference does suggest the possibility of new devices for carrying out terrorist acts, consider the following:

- 1. Most airlines require you to declare whether you have any electrical items in your baggage, and will ask you to remove the batteries (e.g. British Airways, Cathay Pacific)
- 2. Some airlines will not carry unaccompanied baggage (El Al is a pretty good example).
- 3. Some airports require you to turn on electrical devices at the security check to demonstrate that they work normally. At the levels of radiation output suggested, the X-ray/metal detector equipment would probably malfunction, which ought to make the security personnel suspicious.

The ability to circumvent these procedures and successfully smuggle a 'HERF bomb' onto a plane does NOT make HERF interference any more RISKy than other devices which could destroy a plane. Instead, it points to poor execution of security procedures. If an airport's security is really bad, then one could probably smuggle a real bomb on board.

As for a HERF gun aimed at planes taking off - why is this a serious risk beyond that posed by more conventional weapons? A guy standing off the end of the runway with a rifle could probably put enough holes in the fuel tank to cause trouble, and it's easier than building a HERF gun.

>Cyberspace has indeed come of age, and modern airplanes are as much a part >of it as computer networks.

>It's just that the FAA doesn't know what to do about it yet.

>Let's hope they get up to speed quickly. Very quickly.

Current research (of which there is admittedly little) indicates that portable computers are extremely unlikely to be the cause of HERF interference; the FAA would be wise to do a study on the effects of electrical devices on in-flight control systems. The security threat posed by malicious HERF bombs or guns seems no more (or no less) serious than the threat posed by conventional terrorist devices, and certainly does not justify the shock-horror writing style of the original article. There are as many RISKS in creating unnecessary panic as there are in overlooking hazards.

Ted Wong, Cornell University <tmw5@cornell.edu>

HERF Danger to JQ Public

Jack Boatman <c23jrb@kocrsv01.delcoelect.com> Tue, 19 Oct 93 09:06:21 EST

HERF is *high energy*. It doesn't come from laptops, CD players, or FM radios.

My understanding is that HERF comes from the government's testing of directed energy weapons. The characteristics of the directed energy are classified.

Design and test for electromagnetic compatibility is not easy; especially when the electromagnetic environment is not defined. And that is the root of the HERF risk.

BTW: I don't deny that there are risks associated with radio frequency interference from laptops, mobile transmitters, and other electronic devices. I just don't want HERF to be put in the same risk category.

★ Re: Digital Signatures (Smith, RISKS-15.14)

Robert J Woodhead <trebor@foretune.co.jp> Tue, 19 Oct 93 15:02:02 JST

In Risks 15.14, Karl Smith writes (regarding Digital Signatures):

> Well, now the businesses have our number. Our public key identifies us, >uniquely. Nobody else will have the same public key. This means that >businesses no longer have to try to track us down via our SSN or Driver's >license number - they've got a much better number to use to refer to us in >their database - our signature.

Using the same technology, it is possible to create digital pseudonyms that can both assure a retailer of the purchaser's credentials while protecting his or her (or it's) identity. It is even possible to create "digital cash" that can be anonymously handed from person to person, copied ad infinitum, yet spent only once.

A simple example: you register several pseudonyms with a credentials agency; the retailer can present your pseudo to the agency and be told "it's ok, he's

on the up and up." Yet you can give each retailer different pseudos if you so desire

Of course, this requires you to trust the credentials agency; there are other protocols that eliminate this need, but they are more complicated.

| Robert J. Woodhead, Biar Games / AnimEigo, Incs. trebor@forEtune.co.jp | | AnimEigo US Office Email (for general questions): 72447.37@compuserve.com |

Re: Risks of Virtual Reality

"Carolina, Robert" <Robert.Carolina@cchance.co.uk> Tue, 19 Oct 93 10:05:40

The newspaper article you mentioned was published in the *Independent on Sunday* of 4 September 1993. It is probably only fair to point out that on 3 October 1993, the *Independent* printed a clarification. In the first paragraph, they state:

In fact, although Sega is developing virtual reality games for both arcade and home use, the company does not yet have any such games on the market. We accept that any suggestion in our heading that Sega is selling a game which has been found to be potentially damaging to eyesight is misleading. We apologise for any embarrassment caused.

In the second (and last) paragraph:

The company [Sega] also claims that the research [cited in the article] used a prototype with very high powered lenses, designed for a different application, and that the technology is so different that a comparison is not valid.

Robert.Carolina@cchance.co.uk Clifford Chance 200 Aldersgate Street London EC1A 4JJ +44 71 600 1000 (work)

★ Re: Wiretap Laws and Procedures (Leigh, RISKS-15.14)

<smb@research.att.com>
Tue, 19 Oct 93 10:46:56 EDT

This implies that applying a DNR to a suspect's line does _not_ require a court order and is not considered wiretapping. In other words, the list of numbers called by a suspect is not protected as rigorously as the content of those calls. I'd like to hear more about how this data is protected or made available to investigators and others.

Use of ``pen registers'', which record the numbers you dial, or ``trap and trace'' devices, which records who has called you, are regulated by 18 USC 3121-3126. The requirements for court orders are somewhat similar, though at first glance, they're somewhat easier to obtain; as I recall, the wiretap laws

restrict the use of wiretaps to serious crimes, while there's no such provision in the pen register law.

Steve Bellovin

★ Re: Australian government to replace DES (Burfitt, RISKS-15.14)

<smb@research.att.com>
Tue, 19 Oct 93 10:56:43 EDT

Burfitt describes a new Australian encryption algorithm, notes that it runs at 20 Mbps, and asks:

Isn't part of the security with DES its slowness, which implies that this new encryption method will be inherently risky because of its speed?

No, DES was never designed to be slow, though there are some aspects of its design which are inherently quite slow if done in software. You may be thinking of the UNIX system password hashing algorithm, which is based on DES, and which was indeed intended to be slow.

Not that 20 Mbps is particularly fast today. Eberle and Thacker have described a 1 Gbps DES chip (Proceedings of the IEEE 1992 Custom Integrated Circuits Conference), and 40 Mbps chips are readily available.

There is some slight risk in an encryptor being able to run too quickly, in that it makes exhaustive search somewhat more feasible. But key size is a much more important variable. DES's 56 bits are too few; see Wiener's design (CRYPTO '93) for a US\$1 million DES-cracking machine, or for that matter the Diffie-Hellman critique of DES in 1977 on just those grounds.

In evaluating this new algorithm, I'd look at the key size, whether or not the algorithm is open to public scrutiny, and whether or not the Australian government is fond of things like key escrow.

Steve Bellovin

★ Re: Software safety on UK national news (RISKS DIGEST 15.13)

Pete Mellor <pm@csr.city.ac.uk> Fri, 15 Oct 93 10:43:55 BST

In <u>RISKS DIGEST 15.13</u>, Jonathan.Bowen <Jonathan.Bowen@prg.ox.ac.uk> writes:

- > The Wednesday 13th October 9 o'clock evening news on BBC1 TV in the UK > featured a new report from the UK HSE (Health and Safety Executive) ...
- > ... Does any RISKS reader have a full reference for the report?

>From a telephone call to the HSE information centre just now, I gather that the news report probably referred to the latest issue of "Statement of Nuclear

Incidents at Nuclear Installations", which is a regular quarterly report.

It can be obtained free by post (at least in the UK) by telephoning the London Information Office of HSE on: +44 (71) 243 6385

Other useful numbers:

Main HSE Information Office: Tel.: +44 (742) 892345

Fax.: +44 (742) 892333

Main HSE Publications Orders: Tel.: +44 (787) 881165

I should warn readers that none of the people to whom I spoke were sure exactly to which report the news item referred.

Although they are not relevant to the original topic, readers may also be interested in the following publications of HSE:

Guidance leaflet on safety of Visual Display Units (free from London office).

"Display Screen Equipment Work: Guidance on Regulations", ISBN 0 11 886331 2, available also from any Dillon's bookshop, price: 5 pounds sterling. This is a guide to the EEC regulations which came into force in Jan. 93.

"Programmable Electronic Systems in Safety Related Applications", in two parts:

- 1. An Introductory Guide, ISBN 0 11 883913 6
- 2. General Technical Guidelines, ISBN 0 11 883906 3

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V OHB, Tel: +44(0)71-477-8422, JANET: p.mellor@csr.city.ac.uk

Re: Libraries and Imagined Communities

<Bruce_Hamilton.LAX1B@xerox.com>
Fri, 8 Oct 1993 16:52:38 PDT

I think that far too much is made of the supposed "imagined communities" of readers that exist today. I never read the LA Times sports section; other readers probably read ONLY the sports section. Even specialized journals contain very few articles which are of interest to *all* readers.

We associate with people we like and who already tend to share common mindsets. By word-of-mouth we refine our knowledge and opinions. I believe that the shattering, enabled by Internet, of age- and geography-based ghettos, is far more important than whatever new limitations might be imposed by a-priori electronic information filtering.

I welcome the day when both source and destination filters are so refined that I open with pleasure all of my "junk" mail, and I no longer have bookshelves full of magazines and journals where 80% of the content is of no interest to me. I'm confident that personal contacts plus "news flash" features, "best of"

anthologies, and the ramblings of a few favorite columnists (Jerry Pournelle, Dave Barry, P.J. O'Rourke, Ann Landers,...) are quite sufficient to bring any truly important items past any electronic filters.

--Bruce BHamilton.LAX1B@Xerox.COM 310/333-3538

Re: Separating parts in privileged applications

<Bob_Frankston@frankston.com> Sat, 9 Oct 1993 01:06 -0400

There was a good discussion of the Multics ring structure in the new (this year) ALT.OS.MULTICS discussion (we don't give up easily!). What was interesting was that the revisionist view is that rings were not all that useful. Rings were useful internally to provide a supervisor and supersupervisor (kernel) mode and a user mode, though they were overkill for that purpose. Nontrivial attempts to use rings ran up against the mutually suspicious subsystem problem. Similarly the hardware pointer validation was insufficient for real applications.

Basically, protecting the operating system is a minor problem as systems become more complex and the focus shifts from operating system as master of the universe to the operating system as a nice utility that helps keep the local system intact but the real action is in the interactions between subsystems and physically separate systems.

Separating privileged parts - Ring structures

Tom Thomson <tom@fiveg.icl.co.uk> Wed, 13 Oct 93 16:23:02 BST

Yves_Royer in risks 15.08 only knows one OS that uses privilege rings for protection. When I was young everyone expected that all OS would in future be like that. It's amusing to note that the only manufacturer currently making a substantial profit out "conventional" mainframes is also the only manufacturer offering this style of protection in the system. Maybe the loss of this 30 year old technology from the mainstream of OS development indicates a strange risk: if it was developed in academia so that you can't patent it most of industry will go for a patentable alternative even if that's patently inferior. Tom Thomson tom@fiveg.icl.com P.S. for anyone interested, the manufacturer, mainframe series, and OS referred to above are ICL, Series 39, and VME respectively; 16 ring hardware protection fully exploited by the software, with an OS that's been around for 20 years.



Search RISKS using swish-e

Report problems with the web pages to the maintainer

isks Digest Volume 15: Issue 15	Volume 15: Issue 15					



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 16

Tuesday 19 October 1993

Contents

- Social Psychology & INFOSEC Mich Kabay
- Info on RISKS (comp.risks)

Social Psychology & INFOSEC

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 19 Oct 93 05:15:29 EDT

SOCIAL PSYCHOLOGY AND INFOSEC:

Psycho-Social Factors in the Implementation of Information Security Policy

M. E. Kabay, Ph.D.

Director of Education, National Computer Security Association Carlisle, PA

President, JINBU Corporation P. O. Box 509 / Westmount, QC H3Z 2T6 Canada

Internet: 75300.3232@compuserve.com

INTRODUCTION

Security policies and procedures affect not only what people do but also how they see themselves, their colleagues and their world. Despite these psychosocial issues, security personnel pay little or no attention to what is known about social psychology. The established principles of human social behaviour have much to teach us in our attempts to improve corporate and institutional information security.

Information security specialists concur that security depends on people more than on technology. Another commonplace is that employees are a far greater threat to information security than outsiders.

It follows from these observations that improving security depends on changing beliefs, attitudes and behaviour, both of individuals and of groups. Social psychology can help us understand how best to work with human predilections and predispositions to achieve our goals of improving security:

- o research on social cognition looks at how people form impressions about reality (knowing these principles, we can better teach our colleagues and clients about effective security);
- work on attitude formation and beliefs helps us present information effectively and so convince employees and others to cooperate in improving security;
- o scientists studying persuasion and attitude change have learned how best to change people's minds about unpopular views such as those of the security community;
- studies of factors enhancing prosocial behaviour provide insights on how to foster an environment where corporate information is willingly protected;
- o knowledge of the phenomena underlying conformity, compliance and obedience can help us enhance security by encouraging compliance and by protecting staff against social pressure to breach security;
- o group psychology research provides warnings about group pathology and hints for working better with groups in establishing and maintaining information security in the face of ingrained resistance.

The following discussion is based on well-established principles of social psychology. Any recent introductory college textbook in this field will provide references to the research that has led to the principles which are applied to security policy implementation. In this paper, references are to Lippa, R A (1990). Introduction to Social Psychology. Wadsworth (Belmont, CA). ISBN 0-534-11772-4.

SOCIAL COGNITION

Schemas are self-consistent views of reality. They help us pay attention to what we expect to be important and to ignore irrelevant data. They also help us organize our behaviour [Lippa, p. 141]. For example, our schema for relations at the office includes polite greetings, civil discussions, written communications, and businesslike clothes. The schema excludes obscene shrieks, abusive verbal attacks, spray-painted graffiti and colleagues dressed in swim suits. It is the schema that lets people tell what is inappropriate in a given situation.

Security policies and procedures conflict with most people's schema.

Office workers' schema includes sharing office supplies ('Lend me your stapler, please?'), trusting your team members to share information ('Take a look at these figures, Sally'), and letting your papers stay openly visible when you have to leave your desk. Unfortunately, sharing user IDs, showing sensitive information to someone who lacks the appropriate clearance, and leaving work stations logged on without protection are gross breaches of a different schema. Normal politeness dictates that when a colleague approaches the door we have just opened, we hold the door open for them; when we see a visitor, we smile politely (who knows, it may be a customer). In contrast, access policies require that we refuse to let even a well-liked colleague piggy-back their way through an access-card system; security policies insist that unbadged strangers be challenged or reported to security personnel. Common sense tells us that when the Chief Executive Officer of the company wants something, we do it; yet we try to train computer room operators to forbid entry to anyone without documented authorization--including the CEO.

Schemas influence what we perceive [Lippa, p. 143]. For example, an employee refuses to take vacations, works late every night, is never late, and is never sick. A model employee? Perhaps, from one point of view. >From the security point of view, the employee's behaviour is suspect. There have been cases where such people have actually been embezzlers unable to leave their employment: even a day away might result in discovery. Saint or sinner? Our expectations determine what we see.

Schemas influence what we remember [Lippa, p. 145]. When information inconsistent with our preconceptions is mixed with details that fit our existing schemas, we selectively retain what fits and discard what conflicts. When we have been fed a diet of movies and television shows illustrating the premise that information is most at risk from brilliant hackers, why should we remember the truth--that carelessness and incompetence by authorized users of information systems cause far more harm than evil intentions and outsiders ever do.

Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues. In light of the complexity of social cognition, our usual attempts to implement security policies and procedures seem pathetically inept. A couple of hours of lectures followed by a video, a yearly ritual of signing a security policy that seems to have been written by Martians—these are not methods that will improve security. These are merely lip service to the idea of security.

According to research on counter-intuitive information, people's judgement is influenced by the manner in which information is presented. For example, even information contrary to established schemas can be assimilated if people have enough time to integrate the new knowledge into their world-views [Lippa, p. 148]. It follows that security policies should be introduced over a long time, not rushed into place.

Preliminary information may influence people's responses to information presented later. For example, merely exposing experimental subjects to a list of words such as `reckless' or `adventurous' affects their judgement

of risk-taking behaviour in a later test. It follows that when preparing to increase employee awareness of security issues, presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

Pre-existing schemas can be challenged by several counter-examples, each of which challenges a component of the schema [Lippa, p. 153]. For example, prejudice about an ethnic group is more likely to be changed by contact with several people, each of whom contradicts a different aspect of the prejudiced schema. It follows that security awareness programs should include many realistic examples of security requirements and breaches. Students in the NCSA's Information Systems Security Course have commented on the unrealistic scenario in a training video they are shown; a series of disastrous security breaches occur in the same company. Based on the findings of cognitive social psychologists, the film would be more effective for training if the incidents were dramatized as occurring in different companies.

Judgements are easily distorted by the tendency to rely on personal anecdotes, small samples, easily available information, and faulty interpretation of statistical information [Lippa, p. 155-163]. Basically, we humans are not rational processors of factual information. If security awareness programs rely strictly on presentation of factual information about risks and proposed policies and procedures, they will run up against our stubborn refusal to act logically. Security program implementation must engage more than the rational mind. We must appeal to our colleagues' imagination and emotion as well. We must inspire a commitment to security rather than merely describing it.

Perceptions of risks and benefits are profoundly influenced by the wording in which situations and options are presented [Lippa, p. 163]. For example, experimental subjects responded far more positively to reports of a drug with `50% success' than to the same drug described as having `50% failure.' It follows that practitioners should choose their language carefully during security awareness campaigns. Instead of focusing on reducing failure rates (breaches of security), we should emphasize improvements of our success rate.

BELIEFS AND ATTITUDES

Psychologists distinguish between beliefs and attitudes. `A belief ... refers to cognitive information that need not have an emotional component....' An attitude refers to `an evaluation or emotional response....' [Lippa, p. 238]. Thus a person may believe that copying software without authorization is a felony while nonetheless having the attitude that it doesn't matter.

Beliefs can change when contradictory information is presented, but some research suggests that it can take up to a week before significant shifts are measurable. Other studies suggest that when people hold contradictory beliefs, providing an opportunity to articulate and evaluate those beliefs may lead to changes that reduce inconsistency. These findings imply that a new concern for corporate security must be created by exploring the current

structure of beliefs among employees and managers. Questionnaires, focus groups, and interviews may not only help the security practitioner, they may actually help move the corporate culture in the right direction.

An attitude, in the classical definition, 'is a learned evaluative response, directed at specific objects, which is relatively enduring and influences behaviour in a generally motivating way' [Lippa, p. 221]. The advertising industry spends over \$50B yearly to influence public attitudes in the hope that these attitudes will lead to changes in spending habits--that is, in behaviour.

Research on classical conditioning suggests that attitudes can be learned even because of simple word association [Lippa, p. 232]. If we wish to move our colleagues towards a more negative view of computer criminals, it is important not to portray computer crime using positive images and words. Movies like Sneakers may do harm indirectly by associating pleasant, likeable people with techniques that are used for industrial espionage. When teaching security courses, we should avoid praising the criminals we describe in case studies.

One theory on how attitudes are learned suggests that rewards and punishments are important motivators. Studies show that even apparently minor encouragement can influence attitudes. A supervisor or instructor should praise any comments that are critical of computer crime or which support the established security policies. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

PERSUASION AND ATTITUDE CHANGE

Persuasion--changing someone's attitudes--has been described in a terms of communications [Lippa, p. 258]. The four areas of research include

- o communicator variables: who is trying to persuade?
- o message variables: what is being presented?
- o channel variables: by what means is the attempt taking place?
- o audience variables: at whom is the persuasion aimed?

Attractiveness, credibility and social status have strong effects immediately after the speaker or writer has communicated with the target audience; however, over a period of weeks to a month, the effects decline until the predominant issue is message content. We can use this phenomenon by identifying the senior executives most likely to succeed in setting a positive tone for subsequent security training. We should look for respected, likeable people who understand the issues and sincerely believe in the policies they are advocating.

Fear can work to change attitudes only if judiciously applied. Excessive emphasis on the terrible results of poor security is likely to backfire,

with participants in the awareness program rejecting the message altogether. Frightening consequences should be coupled immediately with effective and achievable security measures.

Some studies suggest that presenting a balanced argument helps convince those who initially disagree with a proposal. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes. The Software Publishers' Association training video, It's Just Not Worth the Risk, uses this technique: it shows several members of a company arguing over copyright infringement and fairly presents the arguments of software thieves before demolishing them.

Modest repetition of a message can help generate a more positive response. Thus security awareness programs which include imaginative posters, mugs, special newsletters, audio and video tapes and lectures are more likely to build and sustain support for security than occasional intense sessions of indoctrination.

The channel through which we communicate has a strong effect on attitudes and on the importance of superficial attributes of the communicator. `Face-to-face persuasion often proves to have more impact than persuasion through the mass media.... [because they] are more salient, personal and attention-grabbing, and thus they often stimulate more thought and commitment to their persuasive messages' [Lippa, p. 264]. Security training should include more than tapes and books; a charismatic teacher or leader can help generate enthusiasm for--or at least reduce resistance to--better security.

Workers testing cognitive response theory [Lippa, p. 289] have studied many subtle aspects of persuasion. For example, experiments have shown that rhetorical questions (e.g., `Are we to accept invasions of our computer systems?') are effective when the arguments are solid but counter-productive when arguments are weak.

In comparing the central route to persuasion (i.e., consideration of facts and logical arguments) with the peripheral (i.e., influences from logically unrelated factors such as physical attractiveness of a speaker), researchers find that the central route 'leads to more lasting attitudes and attitude changes....' [Lippa, p. 293].

As mentioned above, questionnaires and interviews may help cement a favourable change in attitude by leading to commitment. Once employees have publicly avowed support for better security, some will begin to change their perception of themselves. As a teacher of information security, I find that I now feel much more strongly about computer crime and security than I did before I created my courses. We should encourage specific employees to take on public responsibility for information security within their work group. This role should periodically be rotated among the employees to give everyone the experience of public commitment to improved security.

PROSOCIAL BEHAVIOUR

Studies of how and why people help other people have lessons for us as we work to encourage everyone in our organizations to do the right thing. Why do some people intervene to stop crimes? Why do others ignore crimes or watch passively? Latane and Darley (Lippa, p. 493) have devised a schema that describes the steps leading to prosocial behaviour:

- o People have to notice the emergency or the crime before they can act. Thus security training has to include information on how to tell that someone may be engaging in computer crime.
- o The situation has to be defined as an emergency--something requiring action. Security training that provides facts about the effects of computer crime on society and solid information about the need for security within the organization can help employees recognize security violations as emergencies.
- o We must take responsibility for acting. The bystander effect comes into play at this stage. The larger the number of people in a group confronted with an emergency, the slower the average response time. Larger groups seem to lead 'to a diffusion of responsibility whereby each person felt less personally responsible for dealing with the emergency' [Lippa, p. 497]. Another possible factor is uncertainty about the social climate; people fear 'appearing foolish or overly emotional in the eyes of those present.' We can address this component of the process by providing a corporate culture which rewards responsible behaviour such as reporting security violations.
- o Having taken responsibility for solving a problem, we must decide on action. Clearly written security policies and procedures will make it more likely that employees act to improve security. In contrast, contradictory policies, poorly-documented procedures, and inconsistent support from management will interfere with the decision to act.

Another analysis proposes that people implicitly analyze costs of helping and of not helping when deciding whether to act prosocially. The combination of factors most conducive to prosociality is low cost for helping and high cost for not helping. Security procedures should make it easy to act in accordance with security policy; e.g., there should be a hot-line for reporting security violations, anonymity should be respected if desired, and psychological counselling and followup should be available if people feel upset about their involvement. Conversely, failing to act responsibly should be a serious matter; personnel policies should document clear and meaningful sanctions for failing to act when a security violation is observed; e.g., inclusion of critical remarks in employment reviews and even dismissal.

One method that does not work to increase prosocial behaviour is exhortation [Lippa, p. 513]. That is, merely lecturing people has little or no effect. On the other hand, the general level of stress and pressure to focus on narrow tasks can significantly reduce the likelihood that people will act on their moral and ethical principles. Security is likely to flourish in an environment that provides sufficient time and support for

employees to work professionally; offices where everyone responds to self-defined emergencies all the time will not likely pay attention to security violations.

Some findings from research confirm common sense. For example, guilt motivates people to act more prosocially. This effect works best 'when people are forced to assume responsibility....' Thus enforcing standards of security using reprimands and sanctions can indeed increase the likelihood that employees will subsequently act more cooperatively. In addition, mood affects susceptibility to prosocial pressures: bad moods make prosocial behaviour less likely, whereas good moods increase prosociality. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them. Even cursory acquaintance with other people makes it more likely that we will help them; it thus makes sense for security supervisors to get to know the staff from whom they need support. Encouraging social activities in an office (lunch groups, occasional parties, charitable projects) enhances interpersonal relationships and can improve the climate for effective security training.

CONFORMITY, COMPLIANCE AND OBEDIENCE

Turning a group into a community provides a framework in which social pressures can operate to improve our organization's information security. People respond to the opinions of others by (sometimes unconsciously) shifting their opinion towards the mode. Security programs must aim to shift the normative values (the sense of what one should do) towards confidentiality, integrity and availability of data. As we have seen in public campaigns aimed at reducing drunk driving, it is possible to shift the mode. Twenty years ago, many people believed that driving while intoxicated was amusing; today a drunk driver is a social pariah. We must move towards making computer crime as distasteful as public drunkenness.

The trend towards conformity increases when people within the group like or admire each other [Lippa, p. 534]. In addition, the social status of an individual within a group influences that individual's willingness to conform. High-status people (those liked by most people in the group) and low-status people (those disliked by the group) both tend to more autonomous and less compliant than people liked by some and disliked by others [Lippa, p. 536]. Therefore the security officers should pay special attention to those outliers during instruction programs. Managers should monitor compliance more closely in both ends of the popularity range. Contrariwise, if security practises are currently poor and we want allies in changing the norm, we should work with the outliers to resist the herd's anti-security bias.

'The norm of reciprocity holds that we should return favours in social relations' [Lippa, p. 546]. Even a small, unexpected or unsolicited (and even unwanted) present increases the likelihood that we will respond to requests. A security awareness program that includes small gifts such as a mug labelled 'SECURITY IS EVERYONE'S BUSINESS' or an inexpensive booklet such as the Information Systems Security Pocket Guide (available from the NCSA) can help get people involved in security.

The 'foot in the door' technique suggests that we 'follow a small initial request with a much larger second request' [Lippa, p. 549]. For example, we can personally ask an employee to set a good example by blanking their screen and locking their terminal when they leave their desk. Later, once they have begun their process of redefinition of themselves ('I am a person who cares about computer security'), we can ask them for something more intense, such as participating in security training for others (e.g., asking each colleague to blank their screen and lock their terminal).

GROUP BEHAVIOUR

Early studies on the effects of being in groups produced contradictory behaviour; sometimes people did better at their tasks when there were other people around and sometimes they did worse. Eventually, social psychologist Robert Zajonc [Lippa, p. 572 ff.] realized that `The presence of others is arousing, and this arousal facilitates dominant, well-learned habits but inhibits nondominant, poorly-learned habits.' Thus when trying to teach employees new habits, it is counter-productive to put them into large groups. Individualized learning (e.g., computer-based training, video tapes) can overcome the inhibitory effect of groups in the early stages of behavioural change.

Another branch of research in group psychology deals with group polarization. Groups tend to take more extreme decisions than individuals in the group would have [Lippa, p. 584]. In group discussions of the need for security, polarization can involve deciding to take more risks--by reducing or ignoring security concerns--than any individual would have judged reasonable. Again, one-on-one discussions of the need for security may be a more effective approach to building a consensus that supports cost-effective security provisions than large meetings.

In the extreme, a group can display groupthink, in which a consensus is reached because of strong desires for social cohesion [Lippa, p. 586 ff.]. When groupthink prevails, evidence contrary to the received view is discounted; opposition is viewed as disloyal; dissenters are discredited. Especially worrisome for security professionals, people in the grip of groupthink tend to ignore risks and contingencies. To prevent such aberrations, the leader must remain impartial and encourage open debate. Experts from the outside (e.g., respected security consultants) should be invited to address the group, bringing their own experience to bear on the group's requirements. After a consensus has been achieved, the group should meet again and focus on playing devil's advocate to try to come up with additional challenges and alternatives.

CONCLUSIONS

By viewing information security as primarily a management issue, we can benefit from the mass of knowledge accumulated by social psychologists. We can implement security policies and procedures more easily by adapting our training and awareness techniques to correspond to human patterns of learning and compliance.

SUMMARY OF RECOMMENDATIONS

- 1. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues.
- 2. Security policies should be introduced over a long time, not rushed into place.
- 3. Presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.
- 4. Security awareness programs should include many realistic examples of security requirements and breaches.
- 5. We must inspire a commitment to security rather than merely describing it.
- 6. Emphasize improvements rather than reduction of failure.
- 7. A new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers.
- 8. Do not to portray computer crime using positive images and words.
- 9. Praise any comments that are critical of computer crime or which support the established security policies.
- 10. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.
- 11. Identify the senior executives most likely to succeed in setting a positive tone for subsequent security training.
- 12. Frightening consequences should be coupled immediately with effective and achievable security measures.
- 13. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes.
- 14. Security awareness programs should include repeated novel reminders of security issues.
- 15. In addition to tapes and books, rely on a charismatic teacher or leader to help generate enthusiasm for better security.
- 16. Encourage specific employees to take on public responsibility for information security within their work group.
- 17. Rotate the security role periodically.
- 18. Security training should include information on how to tell that

someone may be engaging in computer crime.

- 19. Build a corporate culture which rewards responsible behaviour such as reporting security violations.
- 20. Develop clearly written security policies and procedures.
- 21. Security procedures should make it easy to act in accordance with security policy.
- 22. Failing to act in accordance with security policies and procedures should be a serious matter.
- 23. Enforcing standards of security can increase the likelihood that employees will subsequently act more cooperatively.
- 24. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them.
- 25. Security supervisors should get to know the staff from whom they need support.
- 26. Encourage social activities in the office.
- 27. Pay special attention to social outliers during instruction programs.
- 28. Monitor compliance more closely in both ends of the popularity range.
- 29. Work with the outliers to resist the herd's anti-security bias.
- 30. Include small gifts in your security awareness program.
- 31. Start improving security a little at a time and work up to more intrusive procedures.
- 32. Before discussing security at a meeting, have one-on-one discussions with the participants.
- 33. Remain impartial and encourage open debate in security meetings.
- 34. Bring in experts from the outside when faced with groupthink.
- 35. Meet again after a consensus has been build and play devil's advocate.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 17

Thursday 21 October 1993

Contents

A chip, off the old block

PGN

Fiber Optic Cable "Meltdown" in Connecticut

E.M. Culver

NII confidential report "on sale"

Martyn Thomas

US Has It Too (Re: Russian Doomsday Device)

Li Gong

Media Explosion => Loss of Community?

Fred Baube

Re: Auto rentals, law suits, and the risks

Jerry Leichter

Dangers of anonymous remailers

anonymous

Privacy Digests

PGN

SunOS and Solaris vulnerabilities

PGN

CERT Advisory

Info on RISKS (comp.risks)

A chip, off the old block

"Peter G. Neumann" < neumann@csl.sri.com> Thu, 21 Oct 93 14:27:27 PDT

A 2.5-year-old boy and his dog wandered off from their home block in Blacktown, near Sydney, but apparently neither of them could figure out how to get home again. The dog wore a tag indicating that he had a microchip implanted by the Australian Animal Registry, which led to identification of the dog's owners, who -- happily -- were the boy's parents.

[From a clipping from the Sydney Morning Herald, 14 Oct 1993, front page, sent to RISKS by Cameron McLaren in Watson's Bay, Australia. This item

provides a nice technology-related success story. Little Arf Anony?]

Fiber Optic Cable "Meltdown" in Connecticut

<EMCULVER@delphi.com>
Wed, 20 Oct 1993 20:20:04 -0400 (EDT)

A couple of weeks ago a SNET (Local telco) fiber optic cable was found to have been "melted" near where it crosses the Housatanic River. This degraded in-state long distance service and caused the 911 services in several towns, possibly to the New York border (the paper never said) to fail. My brother is a network maven at a local bank. He got some more information:

The papers reported the cable was "melted". The cable was several feet under ground; evidence of a campfire was reported. Must have been one Hell of a campfire!

The telco is certainly not telling all!

NII confidential report "on sale"

Martyn Thomas <mct@praxis.co.uk> Thu, 21 Oct 1993 14:50:34 +0100 (BST)

The report on the Primary protection System for the UK Sizewell B nuclear reactor, from the Nuclear Installations Inspectorate to the Advisory Council on the Safety of Nuclear Installations, is available for two pounds sterling from Computer Weekly, a trade weekly. The report is classified "confidential to members" but the newspaper is selling it "to promote well informed discussion". The report has provoked some controversy in the UK since it was leaked a few weeks ago, because it contains some surprises about the results of the verification activities.

If you want to read a well-written, technical report on the design and verification of a large, real-world safety-critical software system, send your two pounds to Computer Weekly, Sizewell Report, Quadrant House, The Quadrant, Sutton, Surrey SM2 5AS.

Then tell RISKS what you think.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

✓ US Has It Too (Re: Russian Doomsday Device, Kenney, RISKS-15.11)

Li Gong <gong@csl.sri.com> Thu, 21 Oct 93 09:59:19 -0700

In RISKS-15.11, we saw reports (in NY Times, etc.) that Mr. Bruce Blair, a top

US nuclear expert, alleged that the Russians have a Doomsday Device, a computerized system that could automatically launch nuclear strikes even when the Russian leadship is all wiped out. Not noted in RISKS (and also not noted in the San Francisco Chronicle report I saw) are the following two important points (I got these from The Manchester Guardian Weekly, Oct.17, 1993, p.6):

- (1) Blair wrote this in a book, "The Logic of Accidental Nuclear War".
- (2) He also pointed out that the US has things quite similar. For example, the Trident submarines commanders can launch a nuclear strike even when they have lost contact with the US and if they *believe* a nuclear conflict has started.

Someone with access to the book could give us a more complete picture?

Li GONG Email: gong@csl.sri.com Tel: 415-859-3232 Fax: 415-859-2844 SRI International, Computer Science Lab, Menlo Park, California 94025, USA

✓ Media Explosion => Loss of Community?

F.Baube[tm] <flb@flb.optiplan.fi> Wed, 20 Oct 93 23:11:41 EET

There has been concern expressed that when we all stop consuming the same mass media, our shared sense of reality will unravel, with a RISK of bad consequences for social cohesion in general.

That's one way of looking at it.

But consider also that if the technological revolution succeeds in remaking the very nature of the media, from one-way mass transmissions to something more like a community, however many "channels" it may be fragmented into, we all stand to gain more than we lose.

I would like to cite a passage by Jean Baudrillard, critiquing the send-only nature of the mass media. When you think of future media, don't think of home banking and 500 channels of Home Shopping and Gomer Pyle USMC, don't even stop to think of personalized morning newspapers, think of genuinely interactive media where "viewers" (as we would now call them, for lack of a better term) are aware of and can respond to each other -- every channel an encounter.

"The mass media are anti-mediatory and intransitive. They fabricate non-communication -- this is what characterizes them, if one agrees to define communication as an exchange, as a reciprocal space of speech and a response, and thus of a *responsibility* (not a psychological or moral responsibility, but a personal, mutual correlation in exchange). We must understand communication as something other than the simple transmission-reception of a message, whether or not the latter is considered reversible thru feedback. Now, the totality of the existing architecture of the media founds itself on the latter definition: they are always what prevents response, making all

processes of exchange impossible (except in the various forms of response *simulation*, themselves integrated in the transmission process, thus leaving the unilateral nature of the communication intact). This is the real abstraction of the media. [from "Towards a Political Economy of the Sign"]

Fred Baube (tm), GU/MSFS/88 baube@optiplan.fi

Re: Auto rentals, law suits, and the risks

Jerry Leichter <leichter@lrw.com> Tue, 19 Oct 93 23:26:26 EDT

RISKS recently included a discussion of the increasing use by car rental agencies of computer queries of motor vehicle department databases in order to deny car rentals to bad drivers. At least one writer suggested that a law to make any collectors of such data responsible for errors would help keep the error rate under control. It's easy to see this as (a) yet another item on the list of databases that will go wrong because databases *always* go wrong; (b) yet another risk and inconvenience that will be imposed on everyone by the evil users of databases; (c) yet another thing that needs regulation. But it's not that simple. Decisions about databases, from their creation to their maintenance and use, are not purely technical decisions. They are made in a social and legal context, and are affected by a complex set of circumstances. A "quick legal fix" is as unlikely to help as a "quick technical fix".

There's a background to the rental company decisions. Many states have passed laws that make the owner of a vehicle responsible for any damage done with that vehicle. This includes car rental companies. If a car rental company in New York rents a car to Joe Dangerous, and Joe hits Sid Sorry badly injuring him, not only can Sid sue Joe - likely a pointless exercise, as Joe has no assets so is "judgement proof" - but he can also sue the rental company. It makes no difference that the rental company knew nothing about Joe's past driving record; they own the car, they can be held accountable.

In New York, about a year or so ago, after what they claimed were large losses, several of the larger companies announced very large surcharges on cars rented at airports to drivers who lived in certain zipcodes. Needless to say, the zipcodes involved are populated largely by poorer, often minority, residents.

Remember that in judging the risk associated with an action, one must also consider the available alternatives. Screening based on actual driving records, errors and all, is a HUGE improvement. It's quite true that the relatively well-to-do, probably mainly white, readers of RISKS have much more chance of being denied a rental car due to an error in the records in the new system than they did under the older system, which in effect spread the errors uniformly over a less vocal population - or at least a population we are unlikely to hear much from on this list. Still, it seems like a much better trade-off from a social policy point of view.

Finally, on the matter of using lawsuits to curb actions we don't like: This whole mess is an illustration of the complexities. Actions have consequences,

often undesirable ones. It's almost impossible for someone under 25 to rent a car in the US today: They are considered uninsurable at any acceptable rate by the rental companies. The surcharges effectively locked out the poor. Checking of driver's records theoretically locks out those who are really bad drivers - but the criteria used are arbitrary. Two moving violations in the last 3 years? Sorry, no car for you. If you make a business risky enough, it will either vanish or simply become so expensive that it might as well have.

-- Jerry

postings.

✓ Dangers of anonymous remailers

<an32153@anon.penet.fi>
Thu, 21 Oct 1993 01:51:07 UTC

Recently, I asked for information on Usenet, but wanted to remain anonymous, so I used an anonymous remailer to post. Most people have seen anonymous postings, and some people have probably replied to them. What many people probably never think about is the following text at the end of every post (that you will see at the end of my post):

- > Due to the double-blind, any mail replies to this message will be anonymized, > and an anonymous id will be allocated automatically. You have been warned.
- This means that if Bill replies to my anonymous posting, it will go through the remailer and become anonymized. If Bill has sent an anonymous message before, I will receive mail from him with his (permanent) anonymous id. If he puts in his signature at the end of his mail (which I always do when replying to a stranger), he will be giving me his anonymous id with his "real" id. I can then save this information in a database and cross-reference it with any anonymous

In fact, I have been doing just that. I use the "Insidious Big Brother Database" (bbdb) from within emacs, and it automatically inserts email senders into my database, and marks all net-news headers from people in my database. I do this just because I'm curious, not malicious. My database is encrypted, so only I can read it. I could be evil, though.

I could post flame-bait in newsgroups like alt.sexual.abuse.recovery, save all the information from people that flame me, and then post the cross-references to alt.rush.limbaugh. Or I could do worse.

Be careful to whom you reply.																														

To find out more about the anon service, send mail to help@anon.penet.fi. Due to the double-blind, any mail replies to this message will be anonymized, and an anonymous id will be allocated automatically. You have been warned. Please report any problems, inappropriate use etc. to admin@anon.penet.fi.

Privacy Digests

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 19 Oct 93 08:54:12 PDT

Periodically I will remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry general discussions in which risks to privacy are a concern.

* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@vortex.com"; you will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Dennis G. Rears. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated) forum, and was established 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. Submissions should go to comp-privacy@pica.army.mil and administrative requests to comp-privacy-request@pica.army.mil.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing detailed discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN

CERT reports and system breakins

"Peter G. Neumann" <neumann@csl.sri.com> Thu, 21 Oct 93 15:38:02 PDT

The CERT Advisory that follows my message is serious stuff. I tend not to run CERT postings in RISKS, for many of a variety of reasons (e.g., their already-wide distribution, or narrow focus, or sensitivity), but this one seemed particularly relevant to the bigger picture, which is that system and network security stinks in most systems, particularly those on the Internet. Numerous sites have been increasingly experiencing breakins. In addition to

the problems described in the CERT Advisory, many systems have recently had passwords captured from outside intruders using promiscuous-mode Ethernet tapping. This has resulted in the compromise of both incoming and outgoing passwords used for FTPs and TELNETs, for example. Some of these passwords have even been posted for use by others. It is long past high time for system vendors and system administrators to get serious about system/network security. Perhaps the CERT message will serve as yet another reminder, although I have little confidence in things improving very rapidly. PGN]

CERT Advisory - SunOS and Solaris vulnerabilities

CERT Advisory <cert-advisory-request@cert.org> Thu, 21 Oct 93 13:50:31 EDT

CA-93:15 CERT Advisory October 21, 1993

/usr/lib/sendmail, /bin/tar, and /dev/audio Vulnerabilities

The CERT Coordination Center has learned of several vulnerabilities affecting Sun Microsystems, Inc. (Sun) operating systems. Three separate vulnerabilities are described in this advisory. The first and third vulnerabilities affect all versions of SunOS 4.1.x and all versions of Solaris 2.x. The second affects all systems running any version of Solaris 2.x (but does not affect SunOS 4.1.x systems).

Patches can be obtained from local Sun Answer Centers worldwide as well as through anonymous FTP from the ftp.uu.net (192.48.96.9) system in the /systems/sun/sun-dist directory. In Europe, these patches are available from ftp.eu.net in the /sun/fixes directory.

Information concerning specific patches is outlined below. Please note that Sun sometimes updates patch files. If you find that the checksum is different, please contact Sun.

I. /usr/lib/sendmail Vulnerability

This vulnerability affects all versions of SunOS 4.1.x including 4.1.1, 4.1.2, 4.1.3, 4.1.3c, and all versions of Solaris 2.x including Solaris 2.1 (SunOS 5.1) and Solaris 2.2 (SunOS 5.2). Sun is preparing a version of this patch for Solaris 2.3 but no patch ID is available at this time.

** This vulnerability is being actively exploited and we strongly recommend that sites take immediate and corrective action. **

A. Description

A vulnerability exists in /usr/lib/sendmail such that remote users may gain access to affected systems.

B. Impact

Unauthorized access to affected systems may occur.

C. Solution

1. Obtain and install the appropriate patch following the instructions included with the patch.

System Patch ID Filename BSD Solaris
Checksum Checksum

SunOS 4.1.x 100377-07 100377-07.tar.Z 36122 586 11735 1171 Solaris 2.1 100840-03 100840-03.tar.Z 01153 194 39753 388 Solaris 2.2 101077-03 101077-03.tar.Z 49343 177 63311 353

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris, /usr/ucb/sum) and from the SVR4 version that Sun has released with Solaris (/usr/bin/sum).

II. Solaris 2.x /bin/tar Vulnerability

This vulnerability exists in all versions of Solaris 2.x including Solaris 2.1 and Solaris 2.2. Information about patches for current versions of Solaris is described below. Sun is preparing a patch for the upcoming Solaris 2.3 release. The patch ID will be 101327-01, and it will be available as soon as Solaris 2.3 is shipped.

This vulnerability does not exist in SunOS 4.1.x systems.

A. Description

A security vulnerability exists in /bin/tar such that tarfiles created using this utility may incorporate portions of the /etc/passwd file.

B. Impact

Usernames and other information from /etc/passwd and /etc/group may be disclosed. However, since Solaris 2.x uses shadow passwords, encrypted passwords should not appear in /etc/passwd and therefore should not be disclosed by this vulnerability.

C. Solution

We recommend that all affected sites take the following steps to secure their systems.

 Obtain and install the appropriate patch following the instructions included with the patch.

System Patch ID Filename BSD Solaris
Checksum Checksum

Solaris 2.1 100975-02 100975-02.tar.Z 37034 374 13460 747 Solaris 2.2 101301-01 101301-01.tar.Z 22089 390 4703 779

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris, /usr/ucb/sum) and from the SVR4 version that Sun has released with Solaris 2.x (/usr/bin/sum).

- If your site is not using shadow passwords, we recommend that all passwords be changed, especially those for sensitive accounts such as root.
- 3. Depending upon the sensitivity of the information contained in the /etc/passwd file, sites may wish to replace existing tar files where this is possible. Restoring an existing archive file, and then producing a new tarfile with the patched tar, will result in a clean archive file.

III. /dev/audio Vulnerability

This vulnerability affects all Sun systems with microphones. This includes all versions of SunOS 4.1.x including 4.1.1, 4.1.2, 4.1.3, 4.1.3c, and all versions of Solaris 2.x including Solaris 2.1 (SunOS 5.1) and Solaris 2.2 (SunOS 5.2). Sun is addressing this problem in Solaris 2.3.

A. Description

/dev/audio is set to a default mode of 666. There is also no indication to the user of the system that the microphone is on.

B. Impact

Any user with access to the system can eavesdrop on conversations held in the vicinity of the microphone.

C. Solution

To prevent unauthorized listening with the microphone, the permissions of the audio data device (/dev/audio) should allow only the user logged in on the console of the machine to read /dev/audio. To prevent unauthorized changes in playback and record settings, the permissions on /dev/audioctl should be similarly changed.

- *** Any site seriously concerned about the security risks associated with the microphone should either switch off the microphone, or unplug the microphone to prevent unauthorized listening. ***
- 1. Restricting access on 4.x systems

Use fbtab(5) to restrict the access to these devices. See the man page for more information about this procedure.

2. Restricting access on Solaris 2.x systems

To restrict access to these devices to a specific users, the permissions on the device files must be manually changed.

As root:

chmod 600 /dev/audio # chown





Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 18

Weds 27 October 1993

Contents

Saab Story: Cars rolling off the assembly line

Vernon L. Chi

Yet another date overflow bug

David Lamb

OZDISK - Big Brother Down Under?

Mike Bell

Russian Hacker Activity

David Fowler

Thank you

Lauren Wiener

Re: CERT and "security incident" handling

Doug Moran

A. Padgett Peterson

Scott Schwartz

Bruce R. Lewis

Nick Rothwell

Re: The FAA discovers HERF

Dennis Chamberlin

Info on RISKS (comp.risks)

Saab Story: Cars rolling off the assembly line

Vernon L. Chi <chi@cs.unc.edu> Mon, 25 Oct 93 07:39:07 -0400

>From Road & Track, November 1993:

In Sweden, an empty automated Saab factory jump-started itself and assembled 24 cars and rolled them off the assembly line into the factory wall. A worker finally discovered the mishap and found an impressive pile of chrome and steel. A Saab official noted the damage was minimal. 'Our assembly lines run slowly, and we have big bumpers,' he said." I like it. The robustness here was mechanical, and obviously was able to accommodate an unintended run of at least 24 cars without major damage...

[Before most of you were born, a radio comedian named Henry Morgan once had a shtick commercial for a fictitious car manufacturer:

BUSKIRKS are now rolling off the assembly line. We will start delivering them as soon as we can get them BACK ON THE ASSEMBLY LINE.

Ergo, the SUBJECT line, with PGN is delving back into his youth.]

Yet another date overflow bug

David Lamb <dalamb@qucis.queensu.ca> Wed, 27 Oct 1993 13:44:37 GMT

This appeared in comp.os.linux.announce today. It's surely "old hat" to risks readers, who probably remember tales of more egregious date overflows in banking systems in 1969/70 and 1975/6. I suppose that in a "free" operating system like linux, one gets what one pays for -- but I'm a bit discouraged that such simple conventional wisdom as is needed to avoid this escapes most of our practicing programmers.

If you don't use term, read no futher. If you don't know what term is, read no further.

[term is a package which allows you to open multiple sessions over a single modem dialup connection; like a rudimentary SLIP. --mdw]

Well, it had to happen. Sometime on Oct 26th, term died, probably all around the world. The problem is that a variable was defined to be 'int' instead of 'unsigned int', and so, as a result, it overflowed. This caused all the packets to stop being sent. Fun, huh?

Software Technology Laboratory, Computing and Information Science Queen's University, Kingston, Ontario, Canada K7L 3N6 (613) 545-6067

OZDISK - Big Brother Down Under?

Mike Bell <bell@promis.com> Fri, 22 Oct 93 10:04 EDT

This week TV Ontario re-broadcast an Australian documentary "GUMSHOE" which depicted - in fly-on-the-wall format - the work of Australian private detectives.

One of the detectives explained that the greatest changes in recent years have been the mobile phone, and "OZDISK" - a CD-ROM which he then demonstrated.

It allows the user to search and cross-reference by telephone number, street address, and name. It was implied that all the names of people living at an address were indexed.

Among the uses demonstrated: it allows the investigator to identify people living at an address from a phone number; to pretend to be a friend of the neighbours to gain a persons's confidence; to explain a presence in an area.

Presumably it allows con-men, burglars and kidnappers to do the same.

Is this a restricted publication, or can anyone get one? And what organisation is "responsible" for publishing it?

Mike Bell, Leapfrog Software Technology Inc. <71062.3656@compuserve.com> Tel: +1 905 857 4326 Snail: 172 Ridge Rd, Bolton, Ontario L7E 4V4 Canada

Russian Hacker Activity

David Fowler <fowler@oes.ca.gov> Sat, 23 Oct 93 23:35:30 PDT

According to the Associated Press last week, computer hackers nearly succeeded in stealing 68 billion rubles, or about \$57 million, from Russia's Central Bank in August.

The unidentified hackers got into the bank's computer using a random combination of access codes, then tried to transfer the money into accounts at commercial banks. The attempt failed because the thieves lost too much time transferring the vast sums, and the bank detected the computer leak.

Since the beginning of the year, according to the AP, the Russian Central Bank has discovered attempted thefts and fraud totaling about 300 billion rubles, or \$250 million.

This was only the latest in a string of thefts and attempted frauds at the state-run bank since the breakup of the Soviet Union, bank officials said. Bank officials told AP that, last year, thieves stole billions of rubles from the bank using false "avisos," or documents transferring money from one bank to another.

Thank you

Lauren Wiener <lauren@reed.edu> Sat, 23 Oct 93 12:07:34 -0700

Digital Woes: Why We Should Not Depend on Software has been published by Addison-Wesley, and I just wanted to thank everyone who has been posting to comp.risks since 1990. Listening in on this discussion has been a real education for me, and I don't think I could have gotten such an education anywhere else. Thanks to all of you for the honesty, the insight, the frankness, and the intelligence.

-- Lauren Ruth Wiener

"security incident" handling -- comments on CERT's policy

Doug Moran <moran@ai.sri.com> Wed, 27 Oct 93 12:28:03 PDT

The subject of what and how information about computer security problems should and should not be made available has been discussed here and in a variety of other forums. Typically these discussions are in abstract terms, and focusing on the difficulties of balancing competing problems. I have been encouraged to submit the below description of my interactions with CERT (Computer Emergency Response Team) because people who don't deal directly with CERT have been surprised at the extreme position that CERT takes on these matters: it is not much of an exaggeration to say that CERT's position is that they are an input-only channel. Since CERT is being used as a model for similar groups, their approach takes on even wider significance.

My background: I handle part of the management of a cluster of approx 50 Suns. Because my group collaborates with various companies and universities, I wind up getting involved in dealing with breakins at some of those other sites ("collective insecurity" :-)). My site is well-known (we were one of the first sites on the original ARPAnet), and I am known to people at CERT -- I should have no problem getting vetted as trustworthy if CERT were to do that. The following are my personal opinions (not my employers) based on my experiences plus those of the system managers and administrators that I interact with.

Previous Incidents

MO to them.

Over the years, I have dealt with a variety of breakins and attempts. When it was possible to trace the cracker forward or backward, I would send the M.O. (modus operandi = profile) of the cracker (not just the holes that he tried to exploit, but also a list of symptoms that a site should look for). After the creation of CERT, I would also send this

I now regard the minuscule effort needed to send CERT a copy of this MO a waste of time because CERT refuses to provide this information to sites that have been broken into. I have personal experience with this on both sides:

- 1. I have contacted CERT about a particular cracker and given a substantial profile and asked if CERT could tell me anything more about this particular cracker. All CERT has been willing to provide is their generic documents. In backtracking the cracker, I found a site that had identified the cracker's MO and reported it to CERT.
- 2. Similarly, I have been the one to report an MO and later be contacted by a site that had gotten nothing from CERT, but had learned of me by backtracking the cracker to a site that I had contacted.

Current Incident

A site with which mine has substantial interactions was broken into by a cracker in mid-September, and consequently I got involved in helping with the problem. We very quickly found several of his tools and enough other things to constitute a reasonable signature. We contacted CERT and they claimed to have no knowledge of this particular cracker.

The cracker was using captured passwords to daisy-chain from site to site. Unfortunately, we didn't immediately find all the holes and backdoors that he had planted. Consequently, the cracker persisted in having access to that site for some time, thereby having a chance to capture additional passwords. In the followup, we found multiple other sites that had been broken into by the same cracker (coming or going). None of these had gotten any useful information from CERT.

Two days before the recent CERT announcement that there was a hole in sendmail, I got a message from the admins for that site: "he's back". They found a backdoor that he had installed, but were unable to figure out how he had gotten in to install it. Suddenly, with the announcement of the hole, several things we had seen (and reported) seemed to fall into place.

Because this cracker had earlier probed my site from various other places on the net (we had already closed the holes he was exploiting), I was concerned that he might have used this newly found hole to compromise my site (remember, he had broken into a number of the universities and companies with which we collaborate). I called CERT and asked if they could tell me what symptoms to look for to determine whether or not this hole had been used. I was told that there were definite symptoms, but that CERT couldn't tell what they were because that would give away what the hole was. I reminded them that their advisory said

"** This vulnerability is being actively exploited and we strongly recommend that sites take immediate and corrective action. **" and that we had already reported a breakin-in-progress (at the site I was helping), but to no avail. I subsequently got the information I needed from another source, but only at the cost of not being able to pass it on.

One of the many other sites that had been broken into by this same cracker posted to various relevant newsgroups a list of the sites that it had determined to have been compromised (the list was several screens long). CERT posted the following response to those newsgroups:

- > Newsgroups: comp.security.unix,comp.sys.sun.admin,alt.security,
- > comp.security.misc
- > From: cert@cert.org (CERT Coordination Center)
- > Subject: Re: Security Incident -- many sites exposed.
- > Reply-To: cert@cert.org
- > Organization: CERT Coordination Center
- > Date: Tue, 19 Oct 1993 15:51:54 EDT
- >
- > CERT is aware of the incident reported earlier today and we are
- > working to help resolve it. It is CERT policy not to publicly

- > disclose sensitive incident information, particularly names
- > of sites that are, or may have been, involved. Therefore, we will not
- > post the list of affected sites here or on any other netnews group.

>

- > We are reviewing the information concerning this incident and we will
- > endeavor to contact all sites known to be affected within the next
- > 24 hours. We would appreciate your patience and ask that you not
- > contact us about the earlier posting, via either e-mail or telephone,
- > so that we can concentrate our resources on contacting and helping the
- > affected sites.

>

> CERT Coordination Center

>From what I can determine, what CERT means by "help" is that they tell the site that they have been broken into and then provide the generic documents on security patches and practices. The sites I have talked to never have gotten information specific to a particular incident.

Note also that this "response" comes more than a month after the first reports to CERT of this cracker (or a very similar one).

Comments

Caveat: since CERT is almost exclusively an input-only channel, it is hard to determine what they knew and when they knew it.

While I agree with the sentiment in CERT's posting above (that it is undesirable to publicly identify sites that have been broken into), I cannot disagree with the action of the site that posted the list of compromised sites -- the cracker seemed to be spreading faster than he was being found and excluded. (Note that I am not identifying the site that I went to help, nor am I free to publicly discuss details).

In my opinion, CERT's policy contributed substantially to the number of sites broken into and the persistence of this cracker on the network. First, when a system administrator contacts CERT and is told that CERT doesn't recognize the pattern of a given breakin, the SysAdmin is likely to believe that he is dealing with an isolated case, either involving a local user or just one or two other sites. The MO of this cracker left little evidence to contradict this view. Consequently, a SysAdmin could easily focus on the wrong containment measures, allowing the cracker to continue to use his site as a base to attack other sites.

Second, because CERT is unwilling to release info on the various tricks and tools that the cracker was using, a SysAdmin could easily stop short in his cleanup, after finding only some of the holes the cracker was using or had installed. This is what happened at the site I was helping. This gave the cracker time to capture passwords needed to daisy-chain to other sites. Similarly, since CERT refuses to give any advice on what holes the cracker might be using, the SysAdmin may well spend his time and efforts closing holes that aren't currently being exploited, giving the cracker time to further compromise that site and others.

CERT would seem to be a classic RISKy system -- because it doesn't behave the way people think it does/should, it causes people to take the wrong actions, especially during crises. And the classic way to deal with such a system is to teach people to ignore it.

-- Douglas B. Moran

✓ CERT Reports and system breakins (PGN in RISKS-15.17)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Fri, 22 Oct 93 08:44:44 -0400

>... but this one

>seemed particularly relevant to the bigger picture, which is that system and >network security stinks in most systems, particularly those on the Internet.

I tend to agree. System security which is based on a username/password evidences a single point failure, partially caused by the Internet mail scheme which, unless certain simple steps are taken, passes a fully formed account username/address in the mail header.

Over the last several months, I have been examining the situation and have come to the conclusion that there is a relatively simple means to add another layer of security that, for some reason, no one seems to use.

Back in antediluvian times, we had mainframes with terminals connected directly to ports. By which port was accessed, we knew exactly where the user was. Then cam networks and "virtual terminals". Suddenly we no longer knew where the terminal was that the access request was coming from.

With Ethernet however, every packet contains two basic addresses (TCP/IP adds two more IP addresses but that is a software fiction). These six-byte hardware addresses are burned into firmware and every card has a unique address. Originally administered by Xerox, this address consists of a three byte manufacturer's field followed by a three byte serial number. It would be very difficult (well, nothing is impossible but this would be close) for software to forge an address using commercial equipment and collisions should be obvious.

Given this number and a database to correlate the ethernet address to a particular system/location, it is possible to identify not only the user with conventional means, but also determine whether the access is from a known terminal. Further, since manufacturer IDs are unique also, if the address starts with 00:00:C0, one can tell that the terminal is PC based since those cards (Western Digital now SMC) are only used in PCs.

If then, the IP address in use was assigned to a SUN workstation, the system can then determine that something funny is going on.

More common applications would be for designation of "secure" and "insecure" terminals, refusal of certain information classes to PCs, automatic

software updates by system number. The list goes on.

The unfortunate situation is that it was like pulling teeth to find first a good listing of addresses/owners (Michael A. Patton's listing from MIT - available from FTP.LCS.MIT.EDU with the name pub/map/EtherNet-codes - is the best I found), and secondly how to extract that information in a reasonable manner (Ralf Brown's "Interrupt List" will have some new entries in the next issue), but it can be done - and not just by a sniffer.

As a Proof of Principle, I put together a small .COM file that can be used as part of the login script for a Novell server to retrieve the hardware address of a PC client (well, I have PCs at home so...). This can be exported into a database lookup of known systems to identify exactly which system the client is logging in from. The synergy available from having this information should be obvious.

The program is ETHCRD and is FreeWare. It will return the following information:

- 1) Six-byte hardware address of the client's Ethernet card
- 2) Whether a packet (TCP/IP) or Novell (IPX/IPXODI) driver is in use
- 3) The card manufacturer's name

The important news is that It Can Be Done.

Padgett

Re: CERT Advisory - SunOS and Solaris vulnerabilities

Scott Schwartz <schwartz@groucho.cse.psu.edu> Fri, 22 Oct 1993 00:21:09 -0400

I'm surprised to see the /dev/audio thing: It's been discussed on the net for years now. Since the fbtab mechanism is so simple, it's odd that SunOS doesn't ship with it taken care of, and amazing that Solaris has apparently dropped (!!) the mechanism altogether.

Two obvious risks: Sometimes an OS upgrade is actually a downgrade. Lots of other vendors probably have the same vulnerability, but no CERT advisory to nudge them to do something about it.

Re: CERT Advisory - SunOS and Solaris vulnerabilities

Fri, 22 Oct 93 10:25:14 -0400

>Any user with access to the system can eavesdrop on conversations >held in the vicinity of the microphone.

Maybe this has been noted in RISKS before, but ISDN speakerphones are said to have a similar vulnerability.

Bruce R. Lewis Analyst Programmer

MIT Information Systems Distributed Computing & Network Services

Re: CERT Advisory - SunOS and Solaris vulnerabilities

Nick Rothwell <cassiel@cassiel.demon.co.uk> Mon, 25 Oct 1993 18:17:08 +0000

- > 1. Obtain and install the appropriate patch following the
- > instructions included with the patch.

Hmm. If I wanted to hack into a large number of SunOS machines throughout the US, perhaps all I'd have to do is set myself up an FTP site with a reasonably official looking name (I can purchase such through a local Internet provider), disassemble and alter my copy of sendmail, and then forge some mail from CERT to various security newsgroups, saying "there is a problem with all your mail systems, we aren't going to tell you what it is, but install this binary patch anyway because we say so."

My point being that this official-looking CERT Advisory message is implicitly preaching security through obscurity. If someone will tell me what this sendmail vulnerability is, then I can test for it, install a patch, and see if it's fixed (which would give me some confidence that the patch isn't a trojan, since it addresses a discovered weakness). Without such information, I'm not going to do anything to sendmail on my SPARC just because some SWAT team says so.

Nick Rothwell | cassiel@cassiel.demon.co.uk

CASSIEL Contemporary Music/Dance | cassiel@cix.compulink.co.uk

★ Re: The FAA discovers HERF (RISKS-15.14)

Dennis Chamberlin <drchambe@tekig5.pen.tek.com> Thu, 21 Oct 93 17:14:28 PDT

Winn Schwartau's article "The FAA and HERF" could be summarized: "There may be a problem. We don't know anything about it, therefore we'd better act now."

He introduces a fragment of relevant theory that, though truthful, is only sufficient to cause confusion about electromagnetic interference.

"A fundamental axiom of electronics...An electric current creates a magnetic field, which travels at the speed of light in all directions. This is the principle of radio and TV and cell phones. If you stick a wire in the air, and connect it a completed circuit, a magnetic field will induce a current flow."

(more Dr. Science stuff deleted)

True enough, but the resulting induced signals are easily cancelled, shorted, or swamped out by common engineering practices that have been

developed for the very reasons that, for example:

"We live in an electromagnetic sewer, and God knows we shouldn't be playing 'let's not worry about it' with computers flying planes at 37,000 feet."

For example, a coax cable within a magnetic signal field will have about the same signal induced in both in the center conductor and in the shield. Therefore, the interfering signal is almost perfectly cancelled out at the destination. This is one important function of cables. (The article makes no mention of this critical difference between wires and cables.) Other, more powerful techniques are often combined with careful attention to transmission paths.

"Antenna" is not a word that applies to cables. Antennas are not meant to amplify signals but to radiate them. In fact, real antennas are often fed by cables in order to prevent any radiation from taking place other than from the antenna itself. I have never seen a mouse on any computer connected with a wire or antenna.

I got a real laugh out of the description of the mouse and "wire" acting as antenna, and the concern about the shield not ever actually reaching True Earth/Power Company ground. Hm. Seems like the aircraft itself might also have a serious problem here. Perhaps it establishes ground through some sort of satellite link? :) (If anyone cares about the answer to this, please e-mail me.)

The techniques for controlling interference have been advanced right along with the rest of electronic engineering. Had solutions not been developed, interference would have long ago put a stop to further advances in speed, power, sensitivity, and complexity. But now we have everyday examples like car radios (very sensitive receivers) delivering pure and faithful audio within the same vehicle that is powered with an ignition system that delivers wideband 40 000 volt discharges to the plugs. Or, MRI medical imaging systems that utilize probably the strongest magnetic fields in common use, yet are controlled by computers using electronics similar to those in laptop machines.

And, the airplane itself is a mixed and intradependent package of fairly high-power emitters (radio, transponder, radar), together with computers, cables, and sensitive receivers. Airplanes may be susceptible if they are not properly designed, constructed and tested. But no convincing case for susceptibility has been made. (The quoted Newsweek article does not establish susceptibility.)

The statement "from a source close to the FAA" about installation of shielded glass suggests a conspiracy to keep it quiet. It further suggests that money is being spent to protect the FAA employees and their work environment, while ignoring the associated "risk" to airliners and passengers.

His sinister implication completes the stereotype of cheap, fast, cute, word-processed, scare journalism. It would have required only a trivial investigative effort to reveal the unexciting fact that the FAA is aware of the question, but they have not been able to demonstrate or reproduce the symptom. Mr. Schwartau concludes that this is due to deficiencies in the FAA, the equipment, or the investigators themselves.

But the designers of aircraft have anticipated that ground and airborne radar would be a routine part of the operating environment, and took care of that in design and test. FAA towers are not required to fly, and their design constraints are not the same as those of aircraft. Nor do they go through certification testing.

Perhaps the problem is so small, it is not easily seen through the grass. The reason the engineers are having trouble "trying to figure out what's happening" may be that any effect is so slight or rare, there is nothing to observe or measure. And, electromagnetic emission and interference is not exactly a new or faintly-understood science.

The scenarios of RF-terrorists are silly. A terrorist that was both crazy enough and clever enough to build a jammer would almost inevitably be frustrated as his target aircraft just flew off and ignored him.

At any rate, Schwartau's recommendation is to take drastic restrictive action based on non-knowledge. This is insufficient reason for the FAA to take "stronger protective measures" against passenger electronics.

One reason is that more serious things happen nearly every day in commercial air transport, but they generally don't fit into the fear-of-things-thatcan't-be-seen category, so we don't hear of them. Instrument failures, autopilot disconnects, software errors, navigation failures and human error are among the many things that happen with more or less regularity in the huge fleet. Even very adverse failures, such as runaway trim, are part of every crewmembers' recurrent training, but are rarer because they get special attention in design.

A second reason is that way up in the front of the craft is the truly critical but redundant system called the flight crew. A very large proportion of their past and continuing training is directed not at knowing how to fly, but in knowing how (and being able) to fly when lots of things are broken. And almost as important, at recognizing that they *are* broken. So rare, speculative, and non-repeatable cases of of interference are generally not going to cause the crew to freeze and gape wide-eyed as their multiple computers drive them helplessly into the earth.

Air travel and airports are enough of an ordeal already, without further stifling passengers with restrictions that deal with such ghostly "risks". Nonetheless, the FAA has done this when there is a question of catastrophic failure, e.g. loss of control. But Schwartau sees no difference between low-level electrical interference and the integrity of the wing-attach bolts.

And, given the rare and non-repeatable nature of the symptom:

If such a blanket prohibition were effective, how would anyone know?



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 19

Weds 27 October 1993

Contents

Optic fibre fragment kills Telecom worker

Robin Kenny

Lanocaine (sp?)

Bob Frankston

Ethernet addresses as "port" ids

Bob Rahe

File on Four on safety-critical software

Pete Mellor

Cracking feature in the small press

Jim Haynes

Re: FAA and HERF - a pun-ctilio

Peter B Ladkin

Re: Clipper

Fredrick B. Cohen

Re: Chip thefts

Mich Kabay

Re: Dangers of Anonymous Mailers

Steven S. Davis

Re: Swiss AntiViral legislation

Claudio G. Frigerio via Klaus Brunnstein

Computer-Aided Verification (CAV'94)

David Dill

Info on RISKS (comp.risks)

Optic fibre fragment kills Telecom worker

Robin Kenny <robink@hparc0.aus.hp.com> Thu, 28 Oct 93 11:11:39 EST

Not too long ago a Telecom worker in Western Australia was reportedly killed when a fragment of fibre optic glass accidentally got into his blood stream. Remembering this, I was horrified to see at a recent trade show some very casual handling of raw fibre by visitors and sales reps at a stand. Some children were trying to handle the fibre bundle too (I stopped them) The risk

is apparent, in the frenetic effort to "de-mytholise" [demythologize?] technology for the general public, we (industry professionals) unknowingly jeopardise their safety.

Can anyone confirm the Telecom worker report? (RISKS-15.17, `Fiber Optic Cable "Meltdown" in Connecticut' prompted this response, as it is not strictly computing.)

★ Lanocaine (sp?)

<Bob_Frankston@frankston.com> Tue, 26 Oct 1993 15:40 -0400

There was a story on the radio (which is why I can't spell it) about patients dying from incorrect dosages of Lanocaine (sp?) because the syringes for the different dosages look too much alike. It brings to mind the discussion on incorrectly calculated radiation dosages. While one can argue that the computer-based systems are very complex and need to meet high standards, I wonder how the problems of such systems compare with those of more conventional systems. The estimates I've heard about incorrect dosages during normal hospital procedures is very high. (Yes, I'm being vague but I don't have the actual numbers readily available).

Ethernet addresses as "port" IDs

Bob Rahe <bob@hobbes.dtcc.edu> Wed, 27 Oct 1993 19:40:08 EDT

In <u>RISKS 15.18</u>, padgett@tccslr.dnet.mmc.com (A. Padgett Peterson) discusses a scheme for using the ethernet MAC address as a mechanism for verifying location, much like we used to do with hardwired mainframe ports.

Unfortunately, there are two problems here. The first is probably the most damaging - the ethernet address is the address of the transmitting unit ON THAT ETHERNET segment. If the unit is not on that segment and is sending via a router, for example, then the ethernet address will be that of the router's ethernet transmitter, and not the originator's physical address.

As to re-writing the ethernet address in the unit itself, I believe that cicso routers can do that rather easily. I don't have the manuals here at home but I seem to remember that is a functionality that is needed in the DEC world.

Bob

File on Four on safety-critical software

Pete Mellor <pm@csr.city.ac.uk> Sun, 24 Oct 93 21:13:07 GMT The BBC Radio 4 programme "File on Four" last Tuesday was devoted to the subject of safety-critical software.

It discussed the causes of the "software crisis", described a number of the famous recent disasters, and then considered what can be done about it.

The problems that arise with software are due to "complexity", "novelty", and "discontinuity".

Prof. Cliff Jones of Manchester characterised the complexity of software in terms of the number of branch points it may contain, and hence the number of possible paths through it. The combinatorial explosion of possible paths makes exhaustive testing impossible in all but the simplest programs. It may be difficult to achieve with 50 Lines of code and 10 branch points. With 10,000 LOC and the same density of branch points, the testing time would exceed the time elapsed since the big bang. As he pointed out, the Sizewell B Primary Protection System contains 100,000 LOC.

Prof. Bev Littlewood of CSR criticised the tendency of manufacturers to take advantage of the presence of software to make systems perform more and more new functions, so that the soft-centred systems are many times more complex than those they replace, and are also attempting completely novel things, whose consequences may be poorly understood.

Cliff Jones returned to describe the discontinuous nature of digital systems, whereby changing one bit in the internal state or input may cause a vast change in the output. This is in contrast with the "traditional" engineering approach which relies on the fact that, in systems which are governed by the laws of physics instead of the rules of logic, a continuous variation of input leads to a continuous variation of output.

I spoke briefly about the problems of certifying software to a certain numerical level of reliability, with particular reference to avionics systems, where the regulations specifically exclude software from reliability measurement, with the result that manufacturers treat its reliability as 1 for the purposes of calculating overall system reliability.

Martyn Thomas described the guidelines for avionics software as simply exhorting the manufacturer to "try harder" with the more critical stuff.

Dan Hawkes of the CAA pointed out that "do your best" is an approach often used with certain hardware systems on aircraft, and said that software was treated no differently from some hardware.

Martyn was in favour of using formal methods on safety-critical software, and also of qualifying the people who work on it. There are no formal qualifications required before a practitioner may tackle a safety-critical item of software, and yet, as Cliff Jones pointed out, programming productivity has been found to vary by up to a factor of 10 between individuals. "Error-prone" modules are regularly found in industry, and this, Cliff speculated, could be due to their being written by error-prone individuals.

Various disasters were cited, including the recent Gripen crash in Stockholm, and the London Ambulance fiasco. Both have been well covered on the list.

A couple of anecdotes of interest concerned the man who called an ambulance for his mother, who had suffered a stroke. After several hours, he took her to hospital in his own car. The ambulance turned up 10 hours later. The crew of another ambulance radioed base after being sent out on a call and asked why the undertaker had managed to get there before them!

My favourite item concerned the garage owner who specialises in tuning software. He gets the binary from the engine management ROM by mounting it in some harness on his PC. With experience, he is able to spot the data tables containing the engine parameters, and he alters the values. By trial and error, he has found how to undo the "detuning" that is often designed into these systems, and he makes the car give you "... a bigger kick in the back, when you give it some boot!" (or words to that effect!).

Regarding Sizewell B PPS, which was discussed at some length, a "confidential leaked document" had found its way into the producers' hands, and was quoted at length. Presumably, this was the same as the one that was featured on BBC Channel 4 TV news not long ago, and is now being sold for two pounds by Computer Weekly? I'll let you know when I receive my copy! :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V OHB, Tel: +44(0)71-477-8422, JANET: p.mellor@csr.city.ac.uk

Cracking feature in the small press

Jim Haynes <haynes@cats.ucsc.edu> Sat, 23 Oct 93 21:33:10 -0700

This week's (October 21) "Coast Weekly", a Monterey County free entertainment (mostly) paper has an article on "hacking" by staff writer Nicole Volpe. I'll quote part of an introduction from the editorial page.

"While interviewing computer hackers for this issue, it occurred to me that there are a lot of similarities between reporters and cyberpunks - We share a belief in freedom of information, a general suspicion of those in power who operate secretly, and an unfortunate tendency to invade privacy.

This reporter got a taste of what it's like to be on the receiving end of privacy invasion when a hacker I was interviewing handed me a printout of personal information about me that he had retrieved, using nothing more than my home phone number. His reasons were valid enough - he wanted to be sure I was who I said I was. As a reporter I was impressed with the investigation, but on a personal level, it gave me the creeps. It was a lesson they don't teach you in J-school..."

The main article covers the exploits of some crackers in the Monterey area, their concern about the Clipper proposal, some stuff about arrests of crackers in other parts of the country, and an interview with a security man from Metromedia's long distance business. The latter says, "If you picked up the phone a year ago, dialed one digit, and then hung up, I could go back and find out what that one digit was. All the records are stored on magnetic tape." [Balance of message was apparently truncated.]

✗ FAA and HERF - a pun-ctilio

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 27 Oct 93 22:32:49 GMT (Wed)

Dennis Chamberlin, in an otherwise illuminating article, says:

- > And, the airplane itself is a mixed and intradependent package of fairly > high-power emitters (radio, transponder, radar),
- Watt counts as a high-power emitter? I'd be ohm-bliged for amp-lification. The radios (including transponder) in my humble Archer take roughly 7 amps at something approximating 14 volts when transmitting.

Peter Ladkin

[PL actually wrote "appoximating", but I didn't think that was punny, so I corrected it. Appox on both your gausses. What a re-volting development. And, yes, I do have a susceptance for puns. Sorry if my resistance ebbed. I was in a Faraway Cage. PGN]

✓ Re: Clipper

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Wed, 27 Oct 93 05:47:34 PDT

I refer all of the risks readers to a set of articles in the LA Times of 10/3/93 which discusses risks related to the Clipper chip. And to fuel the debate, I add my own comments:

IF we hinge everything on the clipper chip and an enemy breaks it, we are vulnerable at every level. Isn't diversity a good idea for protecting the US combined information assets?

I will be willing to use the clipper chip for all of my encryption IF the NSA, DoD, and ALL US Government applications use the clipper chip for ALL of their encryption as well. Do they really trust it that much? I doubt it.

The NY Times article says the US is considering giving clipper chip keys to other governments so they can monitor our communications as well! Does this mean France will be able to steal our trade secrets? They have already started doing it on airplanes, but now they will be able to do it en-masse at low cost - sponsored by the US Government.

Now that we all know the clipper chip is manufactured by Micronix in Torrence, CA, how long will it be before spies manage to get the design and the 'secret' keys? Do we really believe that security there is good enough to trust our entire national assets to it?

Is the US Government giving a monopoly to Micronix for all cryptography

in the US? Since when do they have that right?

Won't the criminals the government claims to be trying to catch be able to buy encryption from the rest of the world? Even if it's illegal to do so, they are criminals, so they will probably be willing! That means that only the criminals will be able to avoid surveillance designed to only observe criminals.

If there are only a thousand or so legitimate phone taps per year in the US, is it really worthwhile to spend \$26 per chip times a few hundred million chips (over 2 billion dollars) nationwide just to assure 1,000 phone taps? That's 2 million dollars per (phone tap per year)! I would think that for 2 million dollars per criminal, the US Government could come up with a much more effective plan for getting the information they need.

Suppose the NSA is wrong? They've been wrong before! Suppose Clipper becomes not so hard to break because of some mathematical breakthrough? Are they willing to bet the farm on this?

Well, that should get things going - FC

Chip thefts

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>

United Press Intl newswire via CompuServe Executive News Service:

Computer chip manufacturer seeks way to stem theft SANTA CLARA, Calif. (UPI) -- One of the nation's largest manufacturers of computer chips said Friday it will start to put serial numbers on its products in an effort to stem the rising tide of robberies."

This move should make it harder for thieves to sell their loot; one hopes it will therefore make warehouses less attractive targets for the armed gangs who have terrorized Silicon Valley in recent months.

And the problem with stealing chips is that you can't take just one....

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

★ Re: Dangers of Anonymous Mailers

"Steven S. Davis" <ssdavis@dpsc.dla.mil> Wed, 27 Oct 1993 08:51:52 -0400 (EDT)

In Risks 15.17, an32153@anon.penet.fi remarked upon the dangers of including a signature with anonymous postings. It's not quite as absurd as it seems, if someone uses a mailer that appends the signature automatically (I can't imagine that anyone who cared about their anonymity, as opposed to those who just are assigned an anonymous id because they reply to somebody who uses one, would deliberately append a revealing signature). The solution to that, at

least on anon.penet.fi, is simple: The server considers anything after a line beginning with two dashes as a signature and cuts it off (this can be a complication if someone tries to append a document to a message and uses a row of dashes to separate it from the main text). So if you want to send mail anonymously, either dump your signature or be certain it starts with --.

[Also noted by Chris Moore <Chris.Moore@src.bae.co.uk>. PGN]

Re:Swiss AntiViral legislation

Klaus Brunnstein

 stein@rz.informatik.uni-hamburg.d400.de>
 Thu, 21 Oct 1993 16:33:37 +0100

Colleagues and friends, thanks for the very helpful and positively critical comments. I append Mr. Frigerio's reply for your information. Klaus (Oct.21,1993)

PS: Mr. Frigerio will have another fight with lawyers who think that any legislation is dangerous as it may also hurt the "good viruses". I argued that "good viruses" exist only in Dr. Cohen's head, as those applications which he always mentions can be realized by non-replicative methods. Moreover, any auto matic reproduction has an unwished side-effect, as copyrights for any software does only apply to the original (=uninfected) program, so viruses "steal" also legal rights from both the originator and the user (who looses the guarantee, if any, of a working program:-)

>>>>>>> Mr. Frigerio's response <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Thanks to everybody who replied on the subject of Swiss Anti-Virus Legislation.

As somebody noticed there was a word missing in the English translation. It should have been: "... destructs electronically or similarly saved or TRANSMITTED data will..."

The text posted to the net, was a trial to include into the "data damaging" even creation and dealing/circulating computer viruses. The idea behind this, is that the virus itself already carries the malicious intent of his author. Therefore it is dangerous in any circumstance. Actually a virus can not be abused, as the idea of abuse includes the possibility, that a virus can be used in a good way too. As I have been told by specialists, there is no such "good use" of a virus as any unauthorized change of data has the potential of interfering with other data and/or programs in environments, that the virus author did/could not foresee. And even the unauthorized use of storage space is a damage, as this space will not be available for authorized uses of the computer system. Computer virus are an "absolute danger", and as any other dangerous thing (like explosive, poison, radioactive materials or genetic materials in specialized labs) computer virus should not be created or circulated without restrictions.

It has been remarked that in the text there was no word about the requisite intent or requisite knowledge of the committer. This way any BBS sysop would always risk criminal charges, if his BBS carries any virus infected software

but the sysop isn't aware of it.

I apologize for not having told that Swiss Penal Law only considers intentional crimes, if there is no explicit indication that negligent acts are punished too. Therefore according to Swiss Penal Law terminology and system, the text posted to the net only considers who "knowingly and willingly" commits the act. That means that the author of the virus has to know it was a virus, what he created: this is always the case. And who circulates the virus has to know it was a virus and he wanted to circulate it. The knowledge that SW was or carried a virus can be proved easily by the fact that nobody knowingly stores viruses without labeling or marking them in any way, in order not to be infected himself (yes, I know: if there really is somebody so foolish, I have to find another way to prove his knowledge). For BBS a "Virus Directory" containing viruses or virus source codes is evidence enough for the "requisite knowledge and intent". The law does no want to punish accidental distribution of viruses.

The phrase "means destined for unauthorized deletion" has been considered unclear. "Means" certainly includes not only software, but source code (on paper as on disks) too. It has been remarked that it's the classical toolmaker problem: a knife can be used as woodcarver to make a great work, but it might be used by a thug to commit murder. I realized this problem, but would you consider a knife as generally destined to commit murder? Or would you consider explosive as generally destined to create damage? We have to be aware that most items can be used in a legal or abused in an illegal way. Seldom an item can only be used in an illegal way, but computer viruses are such items! I do not speak about software using virus specific reproduction techniques (like "killer viruses" for copyright enforcement or "anti-viruses" supposed to fight viruses) that make data changes with the explicit (contract/license) or implicit (highly probable agreement of the user) authorization of the user. This kind of SW is actually not included in the definition of "means destined for unauthorized deletion, modification, or destruction of data". Therefore you cannot say that Norton Utilities, WipeFile or any other similar general purpose SW or utilities are "destined for unautorized deletion, modification or destruction", although they certainly could be used for this.

The text doesn't say anything about malice, malicious intents or the intent to damage, as these elements are very difficult to prove in trial, if the accused denies any such intention. Actually I considered these subjective elements as not really necessary, as the virus already carries the malicious intent of its author: the malice of the author is proved by his virus, and the malice of somebody circulating the virus is proved, if his knowledge, that he was circulating a virus, is proved.

According to general principles of penal law the site of crime is the main link to charge somebody. If a virus has been created or circulated outside the national borders of Switzerland, Swiss Penal law cannot be applied. But if a virus created outside Switzerland is transferred electronically to Switzerland, the downloader will be held responsible, no matter if he was in Switzerland or abroad, as "importing" as a way to circulate the virus. The "success" of the act will take place in Switzerland. Anyway Art. 7 of Swiss Penal Law follows the principle of territoriality and the "Ubiquitaetsprinzip" (sorry: didn't find the correct English word: an act is considered being committed not only where the committer was, when he started his crime, but

also where the "success" has been realized. Anyway I do consider clarifying this by inserting that "importing" virus is considered as "circulating in any way".

As this crime is prosecuted as soon as police or prosecution authority knows about it (so called "ex officio", there is no need for a specific complaint: a detailed information about a fact is enough to start investigations, no matter where the information came from (e.g. abroad).

There is no doubt, that professional ant-virus specialists and scientists should have access to viruses and be allowed to even create viruses. As long as this is covered by the aim of studying strategies to fight computer viruses, this is OK. I actually planned a system of registering these people with a federal authority (e.g. the IS Security Dptm. at the Swiss Federal Office of Information Technology and Systems or the Ministry of Justice). The posted text would be then need to be completed as follows: "Who, without being registered with the proper federal authority, creates... Only trustworthy individuals, who are professionally or scientifically active in combatting such means, may be registered on demand."

The Swiss legislator is actually not only considering "data damaging" but "hacking", "time theft" and computer fraud too, but these ARE NOT subjects of the discussion in this forum now. The same applies to software piracy, already ruled by another law. I will gladly email/fax the German, French or Italian text of the Penal Law draft to anybody interested. Please do not ask me an English translation of these, as I am not a professional English translator of legal text.

I am aware that the UK and Italy have/are going to have laws allowing to prosecute the creation and circulation of computer viruses. If anybody knows of other countries, may he please let me know in any way and as soon as possible.

On Monday, 25 October 1993, there will a meeting with the Ministry of Justice in order to convince them to propose this to the Parliament. This will be very very difficult, as there generally is very little knowledge on, or concern for the threat through computer viruses. Most people have simply never suffered an attack of computer viruses.

Thanks again for following this item with your comments.

Claudio G. Frigerio

P.S.: Please do not suggest to me to send them a floppy with a just to make them more aware of the risks...

P.P.S.: You can phone/email/fax/write to me in Italian, German, French, Spanish or English.

Claudio G. Frigerio, Bundesamt fuer Informatik/Stabsdienste, Feldeggweg 1, CH-3003 Bern (Switzerland) +41/31/325-9381 bfi@ezinfo.vmsmail.ethz.ch

✓ Computer-Aided Verification (CAV'94)

David Dill <dill@hohum.stanford.edu> Tue, 26 Oct 93 15:01:04 PDT

CALL FOR PAPERS

CONFERENCE ON COMPUTER-AIDED VERIFICATION Stanford University, Stanford CA, USA June 21 - June 24, 1994

This conference is the sixth in a series dedicated to the advancement of the theory and practice of computer-assisted formal verification. Emphasis will be placed on research results that may potentially result in improved techniques, implementation issues for existing verification results, and application of methods to real verification problems.

Special sessions for tutorials and demonstration of verification tools are planned.

The boundaries of the conference are not rigid. In the past, papers on the following topics have been enthusiastically received:

Application areas: synchronous and asynchronous circuits, computer arithmetic, protocols, distributed algorithms, real-time systems, hybrid systems.

Methods based on: automata, model-checking, automated deduction.

Theoretical issues: decidability of verification problems and logics, computational complexity results, verification algorithms.

However, any paper that is of potential interest for computer-aided verification will be considered.

SUBMISSION:

Electronic submission of Postscript(tm) files is REQUIRED, except for authors who do not have reasonable access to electronic mail through Internet, BITNET, etc. Draft papers should be no more than 10 pages long (with normal font sizes, line spacing, margins, etc.) Papers should provide sufficient detail so that their technical contributions can be assessed by members of the program committee. Accepted papers will be published in the conference proceedings. Submissions must be received by January 14, 1994. Authors will be notified of acceptance or rejection by March 11, 1994.

Program Chairman: David L. Dill CIS 135

Stanford, CA 94305-4070

cav@cs.stanford.edu

Steering Committee:

- E. M. Clarke, Carnegie Mellon University, USA
- R. P. Kurshan, AT&T Bell Laboratories, USA
- A. Pnueli, Weizmannn Institute, Israel
- J. Sifakis, Verimag-IMAG, France

Additional members of the program committee:

- R. Alur, AT&T Bell Labs, USA
- R. Brayton, U. of California, Berkeley, USA
- E. Brinksma, U. of Twente, The Netherlands
- R. Bryant, Carnegie Mellon U., USA
- R. Cleaveland, N. Carolina St. U. USA
- C. Courcoubetis, U. of Crete, Greece
- R. de Simone, INRIA, France
- A. Emerson, U. of Texas, Austin, USA
- M. Fujita, Fujitsu, Japan
- S. German, GTE Labs, USA
- O. Grumberg, Technion, Israel
- N. Halbwachs, France
- G. Holzmann, AT&T Bell Labs, USA
- K. Larsen, Aalborg U., Denmark
- K. McMillan, AT&T Bell Labs, USA
- L. Paulson, Cambridge U., United Kingdom
- N. Shankar, SRI International, USA
- F. Somenzi, U. of Colorado, Boulder, USA
- B. Steffen, Techical U. of Aachen, Germany
- P. Varaiya, U. of California, Berkeley, USA
- P. Wolper, U. de Liege, Belgium
- T. Yoneda, Tokyo Inst. of Tech., Japan



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 20

Monday 1 November 1993

Contents

Breakdown in computerised voter support, Oslo

Reidar Conradi

Norwegian hackers fined

\vstein Gulbrandsen

White House distributes STONED 3 virus

Andrew Klossner

Police feedback

Graeme Jones

Taurus Project

E. Kelly

Magnetic Fields in Subway Cars

Bob Drzyzgula

Report on Software Product Liability

Charles Youman

Re: Dangers of Fibre Optic cable

John Gray

Re: CERT Reports and system breakins

Mike Raffety

Re: CERT (was "security incident handling")

A. Padgett Peterson

Re: Ethernet addresses as "port" ids

A. Padgett Peterson

3rd SEI Conference on Software Risk, 5-7 April 1994, Pittsburgh

Ellen Ayoob

Workshop on IT Assurance and Trustworthiness

Marshall D. Abrams

ISOC Symposium on Network and Distributed System Security

Danny Nessett

Info on RISKS (comp.risks)

✓ Breakdown in computerised voter support, Oslo

<Reidar.Conradi@idt.unit.no> Mon, 1 Nov 1993 23:33:25 +0100 Computer error in parliamentary election, Oslo., 13 Sept. 1993

The parliamentary election in Oslo on Monday 13 Sept. 1993 attempted to use a new, computerised system for electorate management ("manntallskontroll" in Norwegian). The system should keep track of electorate composition and participation -- but not what was voted for. By this system, the city hoped to reduce the number of employees from 3000 to 1500 on election day, and planned for that.

The electorate management system was developed since 1988 by the government's computing center (SDS) on a Bull mainframe connected to local PCs. The software had been tried out successfully in smaller elections both in Norway and Denmark, but had not been exposed to a full scale test. It is still unclear who was responsible for this lack of realistic testing -- the city of Oslo or SDS.

However, the electoral management system developed severe "breathing" problems only 1/2 hour after election started at 09:00 on 13 Sept. 1993. It must be said to have effectively broken down, caused by a programming error in the local communication controllers, using character-based instead of line-based transmission protocols.

The error was fixed at 14:00 on election day, but then the municipal election board had already decided to revert to manual backup procedures. These worked reasonably well, all factors considered. In fact, a group of specially invited, international observers from more "low-tech" countries was very impressed by the city's ability for manual improvisation.

However, in the ensuing chaos, there were some irregularities, and 1200 votes had eventually to be discarded or were lost. Therefore, the municipal election board in Oslo unanimously decided to recommend a reelection 2-3 months later. This recommendation was turned down by the newly elected parliament during its own constitution -- in a 119 against 27 vote on 8 Oct. 1993. The reasoning was that the acknowledged election irregularities in Oslo were judged to be insignificant for both the municipal and national election outcomes. On the other hand, a reelection would very likely have caused changes among the elected deputies.

Digression: The ballots were counted optically, *after* all the votes had been cast. The ballots had uniquely punched holes along the paper borders, resembling a punched card. The associated computerised system (also from SDS) worked without problems. However, the right for constituencies (counties) to use entirely electronic voting is still awaiting parliamentary approval ...

Norwegian hackers fined

<oysteing@taskon.no>
Fri, 29 Oct 93 16:45:23 -0100

In Baerum (a small, wealthy area just outside Oslo, the capital of Norway), two hackers were accused of stealing telephone services, and several other forms of fraud. The elder (23) got 18 days suspended and a 2000NKR (300\$) fine

after last year having used a phony name and signed out a modem, and assorted computer-related items from a transport-company. He told the court that he was acting on behalf of another person he got in touch with on a BBS. He was told to check a mailbox (a physical one), and pick up the papers for transport there. He did so, and met with the transport company, identified himself mainly by the acquired papers, and signed out the goods. He paid with a stolen Eurocard-number. He left some of the aquired items on a public place, to be picked up by the other person involved, and kept some for himself. In court it also came out that he used to work at a gas-station, wrote down all credit-card numbers used, and mailed them around the world.

The younger (16) had committed the same scam with the transport-company a couple of times for a "Calvin", which he met on a French BBS. He was fined 2000 NKR (300\$).

None of the boys were sentenced for telecom fraud, on technicalities. The court also found that the boys had been roaming international databases, but did not consider this a computer crime, as they had not destroyed or modified anything. (I personally would like to see a burglar getting of the hook because he did not find anything worth stealing!)

The defendants and their lawyers were very satisfied with the verdict.

\ystein Gulbrandsen Taskon A/S

White House distributes STONED 3 virus

Andrew Klossner <andrew@frip.wv.tek.com> Fri, 29 Oct 93 10:23:19 PDT

Heard on the Rush Limbaugh radio show of 10/29/93, not confirmed:

The White House distributed the 1300-page health care legislation proposal widely on floppy disk. Copies went to legislative staffs and to the press.

It seems that each disk was infected with the STONED 3 virus, which causes a PC to display "Your PC is STONED. Legalize marijuana."

The commentator drew the obvious ironies and puns. (No doubt our esteemed moderator will find non-obvious puns.)

-=- Andrew Klossner (andrew@frip.wv.tek.com)

[People who live in grass browses shouldn't know STONED? PGN]

Police feedback

<JONES_GE_3@prime1.central-lancashire.ac.uk>
Mon, 01 Nov 93 13:27:18

With the CERT-induced issue of passing sensitive information on to those

that could really do with it in mind - I wondered if the British police have an official policy to hand over *all* such information to manufacturers of technical products with exploitable weaknesses. I have been told (don't quote me though!) that for instance, although forged banknote detectors are in use in even our local 20ft by 20ft store, the notes can simply be sprayed with hairspray (one brand works particularly well!) to bypass the ultraviolet light. Similarly, the so-called high security coded car stereos touted at a premium because thieves can't use them can apparently just be placed in the freezer for a while...

Makes me wonder what else clever(?) thieves could achieve if put in charge of a DTI department to boost our exports by undermining foreign products!! Only joking - I've just watched "Rising Sun"...

Graeme

Taurus Project

<EKELLY@dit.ie> Mon, 1 Nov 93 15:17 GMT

In the October 1993 issue of the CACM Inside Risks column, I was surprised that there was no mention of the London Stock Exchange Taurus project which was abandoned in March 1993 after a total expenditure of #400 million pounds sterling (about US\$ 600 million). The British journal "Computing" carried several articles on it. The principle function of the Taurus project, as far as I know, was to computerize the share certificate settlement system.

Magnetic Fields in Subway Cars

Bob Drzyzgula <m1rcd00@frb.gov> Fri, 22 Oct 93 12:47:44 -0400

Commuting on the Washington, D.C. Red Line this morning, I noticed, out of the corner of my eye, something on the floor flash. As I looked closer, I understood that what I saw was a paper clip. But I could have sworn that it moved. A minute later, it did. It stood up on end, about 60 degrees from the plane of the floor. It did this for about 5 seconds, and then fell to the floor again. I watched this go on for about a half an hour... every time the train would accelerate or decelerate, the paper clip would stand up at a rigid 60 degree angle until the train operator disengaged the (electric) drive motors. It probably did this 50 times during my trip. Given that I had some floppy disks in my pack, it made me kind of nervous. And knowing that I have many times, under more crowded circumstances, stood just where that paper clip was (almost exactly in the center of the rail car's floor) with my pack on resting on the floor, I was kind of dismayed. And here I always blamed the cheap floppies my office buys.

So I guess... well, you've been warned.

Bob Drzyzgula rcd@frb.gov

Report on Software Product Liability

Charles Youman <youman@umiacs.UMD.EDU> Sat, 30 Oct 93 21:50:03 -0400

I ran across a report that may be of interest to RISKS readers. It is a SEI report: Software Product Liability (CMU/SEI-93-TR-13) by Jody Armour (School of Law, U. of Pittsburgh) and Watts S. Humphrey (SEI Fellow, Software Engineering Institute). It is available (Postscript, but without figures) via anonymous FTP from ftp.sei.cmu.edu in directory pub/documents/93.reports as file tr13.93.ps. The abstract starts with a reference to an accident involving a radiation machine [Therac 25], although it is not specifically identified, is likely to be an accident already extensively discussed in RISKS, so I have omitted it. The rest of the abstract follows:

Software defects are rarely lethal and the number of injuries and deaths is now very small. Software, however, is now the principle controlling element in many industrial and consumer products. It is so pervasive that it is found in just about every product that is labeled "electronic." Most companies are in the software business whether they know it or not. The question is whether their products could potentially cause damage and what their exposures would be if they did.

While most executives are now concerned about product liability, software introduces a new dimension. Software, particularly poor quality software, can cause products to do strange and even terrifying things. Software bugs are erroneous instructions and, when computers encounter them, they do precisely what the defects instruct. An error could cause a 0 to be read as a 1, an up control to be shut down, or, as with the radiation machine, a shield to be removed instead of inserted. A software error could mean life or death.

★ Re: Dangers of Fibre Optic cable (Kenny, RISKS-15-19)

John Gray <grayjw@cs.aston.ac.uk> Thu, 28 Oct 93 12:48:02 GMT

Robin Kenny mentions the danger of handling optical fibre in RISKS-15.19. I can believe the telecom worker story, but that probably arose from careless handling. "Raw" optical fibre is too brittle for practical use (partly because a fragment snapped from it would be dangerous) so *all* fibres are coated in a flexible plastic coating before they are put onto drums. Thus, what the people were handling is perfectly safe (you need to bend a fibre very tightly before it snaps). Providing the ends of the fibre are not exposed it is safe to handle.

In order to splice fibre ends, you have to strip off the plastic coating, and then any pieces of fibre core which are cut off must be disposed of safely. I

suspect that the Telecom worker concerned was working with the bare, uncoated fibre which is brittle and dangerous.

Possibly the risk of connecting unrelated scenarios? I wouldn't stop children from changing channel on a TV just because a TV service engineer had been electrocuted while servicing one....

John Gray

Re: CERT Reports and system breakins (Peterson, RISKS-15.17)

Mike Raffety <miker@il.us.swissbank.com> Thu, 28 Oct 93 12:44:05 CDT

- > It would be very difficult (well, nothing is impossible but this
- > would be close) for software to forge an address using commercial
- > equipment and collisions should be obvious.

Sorry, it's trivial; every Sun workstation can change its Ethernet address (see the ifconfig command). And in fact, any computer that can do DECnet must be able to do this, since DECnet requires a direct relationship between the Ethernet address and the DECnet address (dumb, but true).

- > Given this number and a database to correlate the ethernet address to a
- > particular system/location, it is possible to identify not only the user
- > with conventional means, but also determine whether the access is from a
- > known terminal.

Sorry, this isn't useful in real life. The Ethernet address will not cross routers; this "solution" would only be useful if both ends of the data flow are on the same network segment (possibly bridged, but not routed).

CERT (was "security incident handling") (Moran, RISKS-15.19)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Thu, 28 Oct 93 09:06:20 -0400

I am not connected with CERT (other than knowing a number of the people involved) and can understand Mr. Moran's position. It is true that generally CERT is "input only" and, while I do not necessarily agree with their position, it is arguable.

CERT does not and cannot provide solutions, they are not funded to do so. It is also their policy not to discuss reported problems other than with the developer of the product in question, and only to produce advisories when a fix for the problem is available.

Having tried to convince manufacturers before that there is a problem, IMHO CERT plays a very necessary role in this matter since CERT does not have to establish credentials.

I do have an advantage over CERT in that, as a hobbyist, I can create and distribute a "fix" with no guarantees or warranties, something neither CERT nor the manufacturer can do (one of the problems with a litigation-happy society). Of course since the "bad guys" enjoy this freedom also, it is a difficult matter. I can state uncategorically that it is *much* more difficult to write an anti-virus program than a virus, much easier to hack/crack than to protect in a manner inoffensive to legitimate users, but then I am egotistical enough to accept those handicaps.

Back to the subject at hand, for example there is currently what I consider a severe problem in Novell Netware 3.x and 4.x that will not be discussed openly just yet since there is no fix. Novell has been contacted and hopefully a new "feature" will soon appear - for Novell the fix should just require a simple change to a single program (maybe 2).

My advantage is that for me this is an ethical choice and not a policy or business dictate, a freedom which neither CERT nor the vendor enjoys. I do know that many people within such organizations do not necessarily agree with such decisions but have no choice in the matter.

Thus I do feel that CERT plays a very valuable role in the process of computer security though it is not often visible as such.

Padgett

★ Re: Ethernet addresses as "port" ids (Bob Rahe, RISKS-15.19)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Thu, 28 Oct 93 09:33:06 -0400

>From: bob@hobbes.dtcc.edu (Bob Rahe)

> Unfortunately, there are two problems here. The first is probably the >most damaging - the ethernet address is the address of the transmitting unit >ON THAT ETHERNET segment. If the unit is not on that segment and is sending >via a router, for example, then the ethernet address will be that of the >router's ethernet transmitter, and not the originator's physical address.

While Mr. Rahe is correct as far as a PING is concerned, the actual packets *must* contain the actual hardware address of the sender in order for the host/server to respond. The fact that the real address may be buried a bit in the packet does not mean that it is not there.

Further, the little .COM program I mentioned runs on the client itself, routing has nothing to do with it, and was designed to be run as part of a login script.

My concept was simple: if all "approved" addresses are known, unapproved addresses are easy to spot. Further, even using the PING method, if I have (and most do) just one or two bridges/routers leaving my reservation then *anything* with their address header should be subject to closer scrutiny.

The problem here is not a matter of too little data but too much (as anyone

who has ever used an unfiltered "sniffer" knows). What I am suggesting is a means of reducing that data to manageable proportions.

Padgett

3rd SEI Conference on Software Risk, 5-7 April, 1994, Pittsburgh, PA

Ellen Ayoob <ea@SEI.CMU.EDU> Mon, 01 Nov 93 15:04:53 EST

Sponsor: Software Engineering Institute

Contact: Julie Walker, SEI, Carnegie Mellon University,

Pittsburgh, PA 15213-3890 phone (412)268-5051 FAX (412)268-5758 e-mail jaw@sei.cmu.edu

Theme: Risk Management in Practice

Please call me if you have any questions or need more information.

Ellen M. Ayoob, (412) 268-6932

Workshop on IT Assurance and Trustworthiness

(Marshall D. Abrams) <abrams@smiley.mitre.org> Mon, 01 Nov 93 16:21:46 EST

****** REQUEST FOR PARTICIPATION ******
Invitational Workshop on
Information Technology (IT)
Assurance and Trustworthiness

March 21-23, 1994 Williamsburg, Virginia

Sponsored by:
Aerospace Computer Security Associates
Co-sponsored by
National Computer Systems Laboratory,
National Institute of Standards and Technology

The purpose of this workshop is to provide input into the development of policy guidance on determining the type and level of assurance appropriate in a given environment. Much of the existing guidance is rooted in the Yellow books, which are based on computer and communications architectures of a prior decade. Technological changes such as local area networks, the worldwide Internet, policy-enforcing applications, and public key cryptography, mandate a review and revision of policy guidance on assurance and trustworthiness.

This invitational workshop is intended to identify the crucial issues and to make recommendations. The audience for the results includes those who deal

with information having sensitivity with respect to national security, privacy, commercial value, integrity, and availability. Potential participants will submit a paper expressing a technical or policy position. These position papers will be used to identify working sessions and to help identify specific participants who should be invited. The submission of the papers and all communication surrounding this workshop will be handled primarily through electronic means. [...]

If you are interested in submitting a paper or just want additional information, please contact Marshall Abrams, abrams@mitre.org.

✓ ISOC Symposium on Network and Distributed System Security

Danny Nessett <nessett@ocfmail.ocf.llnl.gov> Mon, 1 Nov 93 09:50:01 PST

Thursday, February 3 [Breaks etc. removed by PGN]

8:30 A.M.

Opening Remarks

9:00 A.M.

Session 1: Electronic Mail Security, Chair: Steve Kent (BBN)

Certified Electronic Mail, Alireza Bahreman (Bellcore) and Doug Tygar (Carnegie Mellon University), USA

Privacy Enhanced Mail Modules for ELM, Selwyn Russell and Peter

Craig, Queensland University of Technology, Australia

Management of PEM Public Key Certificates Using X.500 Directory

Service: Some Problems and Solutions, Terry Cheung, Lawrence

Livermore National Laboratory, USA

11:00 A.M.

Session 2: Panel: Public Key Infrastructure, Santosh Chokhani (MITRE),

Michael Roe (Cambridge University), Richard Ankney (Fischer, Intl.)

Chair: Miles Smid (NIST)

2:00 P.M.

Session 3: Protocols, Chair: Tom Berson (Anagram Labs)

Paving the Road to Network Security, or The Value of Small Cobblestones,

H. Orman, S. O'Malley, R. Schroeppel, and D. Schwartz, University of Arizona, USA

A Complete Secure Transport Service in the Internet, Francisco Jordan and Manuel Medina, Polytechnical University of Catalunya, Spain 3:30 P.M.

Session 4: Internet Firewall Design and Implementation
Chair: Jim Ellis (CERT)

Inter-LAN Security and Trusted Routers, Pal Hoff, Norwegian Telecom Research, Norway

Trusted to Untrusted Network Connectivity: Motorola Authenticatd Internet Access -- MANIAC(TM), Bill Wied, Motorola, USA

BAfirewall: A Modern Firewall Design, Ravi Ganesan, Bell Atlantic, USA WhiteHouse.Gov: Secure External Access and Service for the Executive Office of the President, Frederick Avolio and Marcus Ranum, Trusted

Information Systems, USA

7:00 P.M. Banquet

Friday, February 4

8:30 A.M.

Session 5: Panel: All Along the Watchtower: Experiences and Firefights Managing Internet Firewalls, Brian Boyle (Exxon Research), Brent Chapman (Great Circle Consulting), Bill Cheswick (AT&T Bell Labs), Allen Leibowitz (Warner-Lambert), Marcus Ranum (TIS)

Chair: Frederick Avolio (TIS)

10:30 A.M.

Session 6: Issues in Distributed System Security

Chair: Cliff Neuman (USC-ISI)

CA-Browsing System -- A Supporting Application for Global Security Services, Denis Trcek, Tomas Klobucar, Borka Jerman-Blazic, and Franc Bracun, Jozef Stefan Institute, Slovenia

The X.509 Extended File System, Robert Smart, CSIRO Division of Information Technology, Australia

Auditing in Distributed Systems, Shyh-Wei Luan (VDG, Inc.) and Robert Weisz (IBM Canada Laboratory), USA/Canada

1:30 P.M.

Session 7: Authentication, Chair: Dave Balenson (TIS)

The S/KEY(tm) One-Time Password System, Neil Haller, Bellcore, USA A Technique for Remote Authentication, William Wulf, Alec Yasinsac, Katie Oliver, and Ramesh Peri, University of Virginia, USA Remote Kerberos Authentication for Distributed File Systems: As Applied to a DCE DFS-to-NFS File System Translator, Thomas Mistretta and William Sommerfeld, Hewlett-Packard, USA

3:30 P.M.

Session 8: Panel: IP Security Alternatives, K. Robert Glenn (NIST), Paul Lambert (Motorola), David Solo (BBN), James Zmuda (Hughes) Chair: Russell Housley (Xerox)

PROGRAM CO-CHAIRS

Russell Housley, Xerox Special Information Systems Robert Shirey, The MITRE Corporation

GENERAL CHAIR, Dan Nessett, Lawrence Livermore National Laboratory

PROGRAM COMMITTEE

Dave Balenson, Trusted Information Systems

Tom Berson, Anagram Laboratories

Matt Bishop, University of California, Davis

Ed Cain, U.S. Defense Information Systems Agency

Jim Ellis, CERT Coordination Center

Steve Kent, Bolt, Beranek and Newman

John Linn, Geer Zolot Associates

Clifford Neuman, Information Sciences Institute

Michael Roe, Cambridge University

Robert Rosenthal, U.S. National Institute of Standards and Technology

Ravi Sandhu, George Mason University

Jeff Schiller, Massachusetts Institute of Technology

Peter Yee, U.S. National Aeronautics and Space Administration

Contact nessett@ocfmail.ocf.llnl.gov (Danny Nessett) for registration and other information, or write ISOC Symposium, C/O Belinda Gish, L-68, Lawrence Livermore National Laboratory, Livermore, CA. 94550.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 21

Tuesday 2 November 1993

Contents

Investment program turns into doomsday machine

Meine van der Meulen

Direct E-Mail: J.S. McBride & Co.

anonymous

"RSI does not exist"

Gavin Matthews

Public relations

Phil Agre

Procrustus

Bob Frankston

Re: Magnetic Fields in Subway Cars

Peter Debenham

Andrew Marchant-Shapiro

Re: Fiber Optic Cable Hazards

Bonnie J Johnson

Re: Breakdown in computerised voter support, Oslo

H?vard Hegna

Re: Ethernet addresses as port ids

Bob Rahe

Virus Security Instituate VSI '94 Announcement

A. Padgett Peterson

ESORICS 94: Call for Papers

Yves Deswarte

Info on RISKS (comp.risks)

Investment program turns into doomsday machine

<MEULEN@tno.nl>

Tue, 02 Nov 1993 13:43 +0100 (MET)

>From the dutch newspaper "De Volkskrant", 2 November 1993:

The investment fund Groeigarant put the "Black Box" out of order. It was designed by Ton Jongbloed, former president of Staal Bankiers, to advise

investors. He claimed on long term it would be twice as profitable as investing in public loans. However the expert system EIS (Electronic Investment Sector) proved to be a "doomsday machine". Only by disconnecting it from the mains larger damage could be averted.

Roughly, the principle of the program was: buy when prices go down, sell when prices go up. This policy was used for several funds selected by Groeigarant. Several months already, prices on the Amsterdam stock market are going up. Therefore, EIS issued orders to sell only. It sold almost all the stocks Groeigarant had, and would have sold even more. The latter would have led to a very risky situation. Selling stocks not available can lead to severe losses when forced to deliver (and having to buy at even higher prices).

Groeigarant says it will base its future investments on fundamental and technical analysis of the stock market. Luckily, the consequences for the fund have been kept to a minimum. Severe losses have been prevented. At the moment the fund mainly possesses money, rather than stocks.

Meine van der Meulen, The Netherlands Organization for Applied Scientific Research TNO, Department of Industrial Safety, meulen@tno.nl.

Direct E-Mail: J.S. McBride & Co.

<[Anonymous]> Mon, 1 Nov 93 10:11:21 xST

According to the Internet Business Report 1.3 (page 4), J.S. McBride and Company are selling access to a database of Internet addresses, including demographic information. They claim over one million entries. The net address is jim_mcbride@netmail.com, and I am sure they would enjoy hearing from anybody who would like to be removed from the list.

[Equifax revisited? PGN]

"RSI does not exist"

Gavin Matthews <GAVIN@shapel.ug.eds.com> Tue, 02 Nov 1993 00:44:16 -0700 (PDT)

The Guardian, 1993-10-29 Friday

Keyboard injury does not exists, judge rules. Angella Johnson

Thousands of keyboards workers suffering the effects of what they believe to be Repetitive Strain Injury were told by a High Court judge yesterday that the condition did not exist. He suggested that keyboard users forced to give up their jobs because of aching muscles and joint were "eggshell personalities who needed to get a grip on themselves".

In a test case ruling that has implications for compensation claims by RSI

victims, Judge John Prosser, QC, declared in the High Court that RSI was meaningless and has "no place in the medical books". He said the condition was more psychosomatic than physical and rejected a claim for damages by journalist Rafiq Mughal against his former employers Reuters news agency.

[There's twice as much again and a followup article `Rulings may only delay claims avalanche' the same length.]

Public relations

Phil Agre <pagre@weber.ucsd.edu> Mon, 1 Nov 1993 22:10:23 -0800

A new article by Oscar Gandy sketches the role of computers in the shifting place of public relations in policy formation in the US, together with some instances of PR affecting policies about information technology. His very useful central concept is the "information subsidy". He points out that many organizations, from the press to the Congress, run on vast amounts of information, but their ability to generate their own information is limited by their budgets. PR people and lobbyists, funded by whoever has enough money and a perceived stake in the outcome, fill the vacuum by supplying information that is customized to fill the organization's needs while simultaneously serving the interests of their patrons. The result is a growing commercialization of the public discourse and the political process, a development with worrisome implications for the cause of democracy. The full reference is:

Oscar H. Gandy, Jr., Public relations and public policy: The structuration of dominance in the information age, in Elizabeth L. Toth and Robert L. Heath, eds, Rhetorical and Critical Approaches to Public Relations, Hillsdale, NJ: Erlbaum, 1992.

Phil Agre, UCSD

✓ Procrustus

<Bob_Frankston@frankston.com> Tue, 2 Nov 1993 04:15 -0400

Two minor incidents this week.

Twice I tried to leave my Sky-Gram phone number as a contact number. Once when getting my car serviced and the other at Children's Hospital. In both cases the data entry field knew what a phone number was and didn't like this silly pin and other commentary. Of course, it would allow any extension number. Or international number. The dark side of data validation and unimaginative implementations.

My kids have hyphenated names. The hospital's system can't, of course, hack hyphens. Neither can airline reservation systems. Can anyone explain this? It's not as if hyphenated names are new. Do systems in the UK exhibit this

kind of silliness?

These observations aren't profound. They just point up the many petty bad design decisions these systems are rife with.

Of course, my trip to the ER pointed out many other disappointments with the DP departments. Analog X-Rays that I had to carry from the pediatrician's to the hospital. The residents on duty had to ask for the same information that the pediatrician already knew. In fact, since I relieved my wife midway through the process, I didn't know the answers as well. If the details were significant they would have affected the treatment. I won't even complain about the amount of time wasted shuffling around. I'll just chalk this up to the risks of nontechnology.

Many readers will, I am sure, applaud the hospital's cautious approach to implementing technology and will point out that I didn't a prescription for a lethal dosage of the wrong medicine. True. But a lack of knowledge can also be dangerous. And wasting time is not a feature.

Re: Magnetic Fields in Subway Cars

Peter Debenham <PMDebenham@email.meto.govt.uk> Tue, 02 Nov 1993 13:36:48 +0000 (GMT)

Following on from the item in Risks15.20, parts of London's Underground system has (or at least 2 years ago had) the same problem of the electromagnetic fields from the trains wiping data from floppy disks. One or two lines were especially bad where the trains differed from the rolling stock on the other lines. Whether the new rolling stock being introduced has solved the problem or made it worse someone else will have to tell. Awareness of the problem was variable.

Peter Debenham, Rm165, APR, Meteorological Office, London Rd., Bracknell, Berks., UK. RG12 2SZ +44 (0)344 856974 pmdebenham@email.meto.govt.uk

★ Re: Magnetic Fields in Subway Cars (Drzyzgula RISKS-15.20)

"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu>
2 Nov 93 08:45:00 EST

In RISKS-15.20, Bob Drzyzgula <m1rcd00@frb.gov> notes his experience with a paperclip while riding on the Washington Metro. While I was in DC last spring, I didn't have much opportunity to move disks around, but I did notice the Metro's emissions. We have a compass in our car (after living in Chicago, navigating in the East requires one!) and I could see it jump all over the place when we were traveling near the Metro; the worst case was when passing OVER the metro tracks.

I'm not at all certain how strong a field is required to change data on a floppy disk; but I will try an experiment this spring, just to satisfy myself that it's safe to travel with my notebook! I must confess that I used to have the same sort of question about the Chicago Elevated system, and that I never had data erased while I was using that to commute; In fact, I've never experienced floppy failure at all; but it sounds like the Metro may be using a different technology in its motors than the El, so it bears investigation...

Andrew Marchant-Shapiro, Depts of Sociology and Political Science, Union College, Schenectady NY 12308 (518) 388-6225 marchana@gar.union.edu

✓ Fiber Optic Cable Hazards

Bonnie J Johnson <COM104@UKCC.uky.edu> Tue, 02 Nov 93 09:55:53 EST

I read with interest the story about the Telecom Worker who had died from accidentally getting a piece of fiber into his bloodstream. Since I didn't see much activity on this list about it, I sent out messages to a Telecom and Safety list.

You see, we pull, rehab and terminate our own fiber here and I certainly want to warn our guys of possible hazards.

Some of the feedback I have received so far includes these:

"This sounds like a hazard which would be encountered in glassblowing shops. Do you have a chem dept. with a glassblower on staff".

"I have been warned that your body does not see glass as a foreign object in the same way that it sees wood for example. So a glass splinter will not itch or irritate, and so it will work into your body. Once there it may meander around and cause fatal problems. I frankly have no idea if this is true, it was a warning given out at a reputable fiber optic termination class. It certainly sounds like a good urban legend material".

"In my graduate fiber optics class, we were warned about this when the prof. passed around some fiber. He told us to be careful to not stick our fingers with the glass, because it was small enough to get into the bloodstream and stop your heart. Now whether this is actually true or just a fiber optic myth/ledgend, I'm not sure. However, I do trust that paticular professor quite a bit. I don't think he told us that just to hear himself think.....".

Anyone one else get any pertinent personal replies they can pass along?

Re: Breakdown in computerised voter support, Oslo

H?vard Hegna <Havard.Hegna@nr.no> Tue, 2 Nov 1993 15:15:04 +0100

Just some comments and clarifications to the message of Reidar Conradi of Nov.1 1993 (RISKS-15.20). Basically the message is correct, but:

1) In Norway voters are automatically "registered" and eligible to vote from the year when they reach 18. They do not have to "pre-register", as is common in the US. The turn-out normally approaches 80 % of the registered voters in the general election. "Electorate management" then is the check at the local polling stations that the voters are in the electorate and that they have not voted before, there or elsewhere. Most polling stations are placed in the local public schools.

Oslo is one of 19 constituencies electing several Members of Parliament (MPs). There are 165 MPs in all, Oslo's 360 000 registered voters elect 16 of them.

- 2) Two computer based electorate systems were used in this election. Both used the schools regular PCs to save costs. The system that failed in Oslo was based on a centralized register, with the PCs acting as terminals. The other system, used in Bergen (the second largest city) was based on local PCs with copies of the full register. This system worked well, but with some unexpected costs. The Norwegian Data Ombudsman insisted that all the PC hard-disks be replaced after the election, so that no copies or shadow disk images of the register could escape. It is basic to Norwegian election laws that no-one shall know who voted. The register itself should, of course, also be under lock and key.
- 3) The Oslo voters had received a voting card shortly before the election. This contained light-pen readable code that greatly simplified checking, provided the system was running. One could of course vote without the card. Proof of one's identity may have to be presented.
- 4) The breakdown in the communication from the schools to the central register occurred because of what was variously called "a programming error in the communication equipment", " a configuration error", "a last minute change for reasons of better performance or functionality", and "a missing full-scale test".

The communication was based on X.25 and the trouble seems to come from a wrong setting of X.3/X.29 PAD parameter 3, "Selection of data forwarding character".

A municipal commission of independent experts now studies the organisation, procedures, user education, and systems of the election from "every angle". It is not yet clear who commissioned the PAD setting, at what time, for what purpose and under which control and testing scheme.

- 5) The Oslo municipal election board did not in fact unanimously recommend a re-election. Based in particular on the fact that 700 votes cast at one of the polling stations, had disappeared, they unanimously voted against sanctioning the result. This left the decision on the question of re-election, to the Parliament. The 700 votes were not lost as a direct result of the computer failure, but probably disappeared in the general confusion after the polling station closed and the counting started.
- 6) All in all, the election was basically under control. Although the municipal administration was clearly too optimistic with respect to the blessings of computer technology, there were enough communication and computer logs, manual backup routines, paper ballots, and envelopes around, to check

whether the final results where within generally acceptable error bounds. Except for the one large loss of votes mentioned above, the errors were small and of the size also expected in a manually run election, according to the administration. They did not add up to an amount that would influence the selection among the candidates.

- 7) The Government proposed last year that a wholly computerized voting system, with Direct Recording Equipment and no paper ballots, could be tested in the 1993 general Election. This was rejected by the Parliament, partly as a consequence of pressure from computer specialists, pointing to the US experience, as reported in RISKS and elsewhere (thank you, all of you). The 1993 experience has done a lot to confirm that rejection.
- 8) An account of the expectations of the project leader for the Oslo election, can be found in the "New Scientist" of Sept.11, 1993. One of the high-lights is the following quote: "An election with only electronic voting can be much more secure and correct than a paper-based one. But we feel the (Parliamentary) committee did not have the necessary knowledge to trust such an advance in the use of technology."
- 9) A personal note: I consider the Oslo election a success, in the sense that it demonstrates wonderfully the necessity of a system of control routines _outside of_ the computer voting equipment. In particular that some form of manually controllable paper ballots be available. A ballot that the voter can read before it is placed in the urn, and that the counting personnel can count manually as a precaution, or if necessary due to a close race, or an equipment failure, or public scepticism. All other forms of control have to be based on computer trust, and on total trust of the computer specialists involved.

As some-one wrote in an Oslo newspaper (Arbeiderbladet, Sept. 28), after the Parliament decided against a re-election:

"Casting one's vote is as close to a sacred act as one can get in a modern democratic secular society. The high-priests of modern technology should be kept at arms length from the more sensitive parts of that act."

Havard Hegna, Norwegian Computing Center, Oslo, NORWAY Havard.Hegna@nr.no (A semi-governmental non-profit computer science research institute)

★ Re: Ethernet addresses as port ids (Peterson, RISKS-15.20)

Bob Rahe <bob@hobbes.dtcc.edu> Tue, 2 Nov 1993 07:55:08 EST

In RISKS-15.20 padgett@tccslr.dnet.mmc.com (A. Padgett Peterson) writes:

|>While Mr. Rahe is correct as far as a PING is concerned, the actual packets |>*must* contain the actual hardware address of the sender in order for |>the host/server to respond. The fact that the real address may be buried |>a bit in the packet does not mean that it is not there.

Well, no, not true. The actual REAL ethernet address of the sender is

lost, from the receiver's point of view, once the packet passes through a router (as another poster mentioned in the same digest). The address that IS passed along inside the packet is the next layer up - the IP address. That address is TOTALLY software driven and thus useless for identifying a port in your scheme.

This discussion sort of assumes TCP/IP over ethernet. As was mentioned, DEC does some things differently and I'm sure there are other schemes, but the ethernet address isn't there past a router. (And lots of systems can change their ethernet address anyway).

I'd suggest Comer's book on TCP/IP for a good discussion of the basics of ethernet and TCP/IP nets.

Virus Security Instituate VSI '94 Announcement

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Tue, 26 Oct 93 10:19:59 -0400

> CONFERENCE ANNOUNCEMENT VSI '94 Philadelphia, Pennsylvania - USA March 29-30, 1994

Presented by the Virus Security Institute
"A Different Kind of Information Security Conference"

VSI '94 -- two intense days of interactive collaboration focused on the development of a working information security model appropriate to both the management and technical challenges of the mid-90s.

Security is not a book of rules; it is an organic and dynamic process. This principle will be expanded through an agressive combination of speakers, scenarios and solutions.

VSI '94 is not a hit-or-miss conference. The program is carefully structured to provide not only state-of-the-art information but practical techniques that "push the envelope".

DAY ONE: In the morning, industry experts will present a limited number of papers dealing with state-of-the-art considerations divided into three areas: scientific, technical, and managerial. This will provide a primer for what is to follow.

In the afternoon, participants will restructure a traditional organization to reflect the information security needs of the mid-90s. The Management Track will address requirements for executives, financial and legal considerations, operating parameters, policies and procedures, re-engineering, communications requirements and a five-year plan. The Technical Track will explore tools and techniques currently available, define requirements and techniques to preserve vital information that may come under attack from any quarter, automation of support functions, necessary networking and risk assessment.

Industry experts in each field will be present to make suggestions and offer examples. The afternoon will be divided into segments for each of the tracks with a focus provided for each. If the participants fail to reach a concensus within the segment's alotted time, the legacy baseline will be used on the next day.

Further planning is encouraged in the bar and at the reception.

DAY TWO: Each of the elements of the restructured model will be examined and challenged, both by speakers and participants. Management will be given legal, financial, and stockholder concerns to address. Technical will defend against attack scenarios ranging from viruses to terrorists to incendiary cows & leaking tunnels.

PLENARY: A recap of the proceedings analyzing strengths and weaknesses of the model as developed, challenged, and improved.

PAPERS: We solicit papers/speakers focusing on the subjects of fiendish attacks, brilliant solutions, organizational indifference, and prognostication. The focus will be on salvation from the Networks (both interpretations apply).

SITE: The entire conference floor of the Philadelphia Airport Hilton has been reserved for VSI '94. Rooms for Birds-of-a-Feather meetings may be reserved in advance, subject to availability. Facilities will be available for larger, lengthy formal meetings on Monday, March 28. The hotel is designed to facilitate "H" (hall) track sessions.

Room Rates: \$72/night, single or double. Contact the Hilton (302)792-2700 The Hilton provides a complimentary continental breakfast to all hotel guests.

TRAVEL: Philadelphia International Airport (transportation from airport provided by the Hilton) is served by most major airlines. Drive time from either Washington, DC or New York is approximately 2 hours. AMTRAK serves Philadelphia's 30th Street Station (local train available every half hour to airport for Hilton pickup). Discounted airfares are available from Sand Lake Travel (800)535-1116 / (407)352-2808 / FAX (407)352-2908

AMENITIES & AMUSEMENTS: Philadelphia is rich in attractions, from the Liberty Bell to the Franklin Institute to the Art Museum to the bustling 9th Street Market. Excellent shopping in both Philadelphia and tax-free Delaware. Nearby is the famous Brandywine Valley, home of Winterthur, Longwood Gardens and Andrew Wyeth. A full activities packet will be available to all registrants.

INFORMATION: For more information, E-Mail or Fax:

EMAIL: VSI94_info@dockmaster.ncsc.mil (case sensitive) FAX: (302)764-6186 (include E-Mail address, please)

Honorary/Convening Chairman - Dr. Harold Joseph Highland, FICS

Conference Chair: Pamela Kane Program Chair: Padgett Peterson PSKane@dockmaster.ncsc.mil Padgett@tccslr.dnet.mmc.com

Founding Members and Directors of the Virus Security Insitute

Vesselin Bontchev

Dr. Klaus Brunnstein

Dr. William Caelli

Jon David

Christoph Fischer

Ross Greenberg

Dr. Harold Joseph Highland, FICS

Pamela Kane

A. Padgett Peterson, P.E.

Yisrael Radai

Fridrik Skulason

Dr. Alan Solomon

✗ ESORICS 94: Call for Papers

Yves Deswarte <deswarte@laas.fr> Tue, 2 Nov 1993 11:25:07 +0100

```
::::: Yves Deswarte - LAAS-CNRS & INRIA - 31077 Toulouse (France) :::::
```

:::: E-mail:deswarte@laas.fr - Tel:+33/61336288 - Fax:+33/61336411 ::::

European Symposium on Research in Computer Security Brighton, United Kingdom, November 7th-9th, 1994

ESORICS-94 (European Symposium on Research in Computer Security) is organised by The IMA in cooperation with AFCET (creator), BCS Security Special Interest Group, and CERT-ONERA.

AIM AND TOPICS: The aim of this symposium is to further the progress of research in computer security by bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in areas related to computer security, information theory and artificial intelligence.

Papers are solicited in the following areas:

- Theoretical Foundations of Security-

security models and specifications, contribution of formal logic and information theory, formal development techniques

- Secure Computer Systems-

operating system security, network security, security management, virus and worms, contribution of artificial intelligence, contribution of new architectures and new technologies

- Security in Data and Knowledge Bases-
- Security in other Applications-

transaction systems, process control, real time, distributed applications

- Cryptography Applications-

authentication, key management, signature

- Security Verification and Evaluation-

formal methods, measure and evaluation of risks, measure and evaluation of security, criteria, protocol verification

- Software Development Environments for Security-
- Operation of Secure Systems-

management, intrusion detection

- Security versus other requirements

Security and costs, performances, dependability, safety, reliability,...

All application fields are welcome (medical, industrial, financial, copyright,...) as long as the proposals remain in the scope of research in computer security.

This list is not exhaustive. Research papers, position papers and panel proposals will be welcomed.

SUBMISSIONS: Six copies of papers or panel proposals should be submitted to the program chair by March 25th, 1994 at the following address:

Gerard Eizenberg
CERT-ONERA ESORICS 94
2, avenue E. Belin
B.P. 4025
31055 Toulouse Cedex
France

The texts must be submitted in English. Papers should be limited to 6000 words, full page figures being counted as 300 words. Each paper must include a short abstract and a list of keywords indicating subject classification. Notification of acceptance will be sent by June 24th, 1994, and camera-ready copies will be due on September 1st, 1994.

Panel proposals should include title, proposed chair, tentative panelists, a 2 or 3 paragraphs description of the subject, format of the presentation, and rationale for the panel.

For further information and/or copy of the advance program when available, send E-mail to Dieter Gollmann at the next address:

dieter@dcs.rhbnc.ac.uk

or write to:

Pamela Irving

Conference Officer

The Institute of Mathematics and Its Applications

16 Nelson Steet Southend-on-Sea ESSEX SS1 1EF United Kingdom

IMPORTANT DATES:

Submission deadline: March 25th, 1994 Acceptance notification: June 24th, 1994 Camera-ready copy due: September 1st, 1994

GENERAL CHAIR: Roger Needham (University of Cambridge, United Kingdom)

PROGRAM COMMITTEE

CHAIR: Gerard Eizenberg (CERT-ONERA, France)
VICE-CHAIR: Elisa Bertino (Universita di Milano, Italy)

Bruno d'Ausbourg (CERT-ONERA, France)

Thomas Beth (Universitaet Karlsruhe, Germany)

Joachim Biskup (Universitaet Hildesheim, Germany)

Peter Bottomley (DRA, United Kingdom)

Yves Deswarte (LAAS-CNRS & INRIA, France)

Klaus Dittrich (Universitaet Zuerich, Switzerland)

Simon Foley (University College, Ireland)

Dieter Gollmann (University of London, United Kingdom)

Franz-Peter Heider (GEI, Germany)

Jeremy Jacob (University of York, United Kingdom)

Sushil Jajodia (George Mason University, USA)

Helmut Kurth (IABG, Germany)

Teresa Lunt (SRI, USA)

Giancarlo Martella (Universita di Milano, Italy)

Catherine Meadows (NRL, USA)

Jonathan Millen (MITRE, USA)

Emilio Montolivo (Fondazione Ugo Bordoni, Italy)

Roger Needham (University of Cambridge, United Kingdom)

Andreas Pfitzmann (Technische Universitaet Dresden, Germany)

Jean-Jacques Quisquater (UCL, Belgium)

Einar Snekkenes (NDRE, Norway)

ORGANISING COMMITTEE

Dieter Gollmann (University of London, United Kingdom)

Pamela Irving (IMA, United Kingdom)



Search RISKS using swish-e

Report problems with the web pages to $\underline{\text{the maintainer}}$



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 22

Friday 5 November 1993

Contents

Direct Subscribers: Can you instead read RISKS as a newsgroup? **RISKS**

Prague computer crime

Mich Kabay

Master of Disaster Phiber Optik sentenced

Mich Kabay

Mass. state police confuse car owners with gun carriers

Brian Hawthorne

Overenthusiastic automated investment programs

John R Levine

RISKS of unaccountable computerized elections

Dave Hart

Re: Safety-critical software

David Parnas

Re: InterNet Mailing List

JS McBride [2]

Security of the internet

Bill Murray

PGN

Yu, "Automated Proofs of Object Code..." available

Jim Horning

"Research Directions in Database Security" ed. by Teresa Lunt

Rob Slade

Re: CERT Reports and system breakins

Phil Karn

A. Padgett Peterson

Call for Participation, FIRST Incident Response Tools Wk Grp

Michael S. Hines

Info on RISKS (comp.risks)

Direct Subscribers: Can you alternatively read RISKS as a newsgroup?

RISKS Forum <risks-request@chiron.csl.sri.com> Fri, 5 Nov 93 16:27:35 PST

Folks, New subscriptions are pouring in at a remarkable rate, and BARFmail is increasing at an even more rapid rate. The network seems flakier than ever. If you are getting RISKS via a direct subscription (check your mail headers), PLEASE check with your local netnews wizards to see if you can now read it as a newsgroup, BBoard item, or local redistribution. If you are able to read it that way, PLEASE do so, and send me a message so that I can remove you from my list (actually plural, multiple lists, because otherise my mail system dies).

[Yes, I know, I should use an automatic LISTSERV, but that creates its own set of headaches. Are there any really robust, moderator-friendly, portable UNIX LISTSERVers I could use for direct mailings of RISKS, despite the fact that I continually get requests from sites that cannot be answered?!*%&!!?]

PGN

Prague computer crime

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 04 Nov 93 17:36:33 EST

CZECH TRANSITION SPURS BOOM IN ECONOMIC CRIME, By Bernd Debusmann PRAGUE, Nov 3 (Reuter, 2 November 1993) - The Czech Republic's transition to a market economy has led to a boom in economic crime ranging from embezzlement to tax evasion, as criminals exploit money-making opportunities denied them under communism.

According to the latest police statistics, economic crime jumped 75.2 percent in the first nine months of the year compared with the same period in 1992 -- a steeper increase than any other criminal activity. [From the Reuter newswire via the Executive News Service (GO ENS) on CompuServe]

The article goes on to state that with the growth of an economy, the opportunities for economic crime are increasing apace. Although police claim to solve 75% of the cases of fraud reported to them, there seem to be many more unreported cases. In a recent case, "Martin Janku, a 23-year-old employee of the Czech Republic's biggest savings bank, Ceska Sporitelna, is accused of transferring 35 million crowns (\$1.19 million) from various corporate accounts to his personal account over an eight-month period."

In a typical hacker's excuse, Janku claims to have done this to demonstrate the bank's poor security. He wrote software himself to be able to tamper with client accounts--but only, he said, after repeatedly warning his bosses of weak security precautions. The theft was not detected by the bank itself until Janku withdrew part of the money. He was arrested as he was in the process of stuffing half a million dollar's worth of banknotes into a briefcase.

The problems of inefficient bureaucracies are compounded by poor laws and indifferent enforcement. The problem is so widespread that about 30% of the residents of Prague own a country home--and a large percentage of those are claimed by analysts to be built through illegal economic activity.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Master of Disaster Phiber Optik sentenced

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 04 Nov 93 17:37:14 EST

Mark Abene, 21, widely known as Phiber Optik, was sentenced to a year and a day in prison. He will serve 600 hours of community service. He pleaded guilty last July to conspiracy, wire fraud and other federal charges relating to his activities as one of five Masters of Disaster indicted for breaking into telephone, educational, and commercial computer systems. [Perhaps in a few years more, they will be Doctors of Disaster?] [PGN Excerpting Service, drawn from the Associated Press and Reuters, both on 3 November 1993]

The Reuter article give background information, including

- o the charges against MoD marked the first use of wiretaps to record both conversations and datacomm by accused hackers.
- o the hackers attacked phone switching computers belonging to Southwestern Bell, New York Telephone, Pacific Bell, U.S. West and Martin Marietta Electronics Information and Missile Group.
- o they broke into credit-status reporting companies including TRW, Trans Union and Information America, stealing at least 176 TRW credit reports.
- o the young men were apparently competing with each other and other hacker groups for "rep" (reputation) and were also interested in harassing people they didn't like.
- o the Reuter article mentions that "they wiped out almost all of the information contained on a system operated by the Public Broadcasting System affiliate in New York, WNET, that provided educational materials to schools in New York, New Jersey and Connecticut" and left the message, ""Happy Thanksgiving you turkeys, from all of us at MOD."

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Mass. state police confuse car owners with gun carriers

SunSelect Strategic Marketing <Brian.Hawthorne@east.sun.com> Fri, 5 Nov 93 13:26:43 EST

My wife received a letter yesterday from the Massachusetts state police, informing her that it was time to renew her "License to Carry Firearms". It included a renewal form that she was to take to her local licensing authority, the police station in our case.

A bit of background: In Massachusetts, a "License to Carry" allows you to carry or transport a handgun. My wife not only has never had such a

license, but does not even have the pre-requisite Firearms ID card, which allows ownership and transport of rifles and shotguns.

Concerned that someone had used her name and address to get a carry permit, my wife called the phone number indicated. The person answering ("State Police") explained that my wife shouldn't worry. Everyone else who got that letter by mistake was also concerned.

They have not yet figured out exactly what happened, but apparently someone loaded a tape containing the list of car owners who needed to renew their automobile registration instead of the list of gun owners needing to renew their carry permits. They generated and mailed many thousands of these letters, and never did any sanity checks.

They assured my wife she would get a letter explaining what had happened as soon as they figured it out.

Fortunately, in order to actually renew a carry permit, my wife would have to present the form in person at the local constabulary, who would know that she did not have such a permit. Unless, of course, someone loaded the wrong tape when updating the local police records...

In retrospect, since a car is a much more dangerous weapon than a handgun, I suppose this is not a very big RISK after all.

✓ Overenthusiastic automated investment programs

John R Levine <johnl@iecc.com> Tue, 2 Nov 93 22:34:05 EST

The story about the Dutch computer that nearly oversold its portfolio reminds me of a similar situation. (This isn't a friend of a friend story -- I actually know the person involved.)

Some years back, he'd been doing some of the earliest experiments in computerized commodity trading. At that point, it was still common to send in orders by Telex, since it left a much better log than did phone calls, and he'd recently gotten a lashup that let his computer make its own Telex calls so it could automatically calculate and enter the day's trading orders.

So the computer put some money into something (potatoes, I think.) The next day, the prices had moved favorably, so it put in some more. Next day, the same thing. Before the end of the week, he got a phone call from the government regulators. The potato futures market isn't all that big, and his computer had apparently cornered it, which is a definite no-no. He unwound his potato positions and adjusted his program never to buy potatoes again, no matter what.

It surprised everyone involved that the computer had been able to distort that market so quickly. Lord only knows what computers do to commodity markets these days; as I recall he managed to do his cornering with a PDP-11.

The general problems with automated trading programs are well known. They had a lot to do with the day the market dropped 500 points, as all of the programs cranked away in a financial environment that their programmers had not really anticipated. There are now "circuit breaker" rules that limit how much automated trading can be done, but I wouldn't place a great deal of faith in claims that computerized market distortions have thereby been cured.

John Levine, johnl@iecc.com, {spdcc|ima|world}!iecc!johnl

RISKS of unaccountable computerized elections

Dave Hart <davehart@microsoft.com> Fri, 5 Nov 93 12:17:38 PST

There's a good article on the risks of computerized election systems which leave no paper trail for recounts in the 30 October 1993 *Science News* [Vol. 144 No. 18 Pg. 282-3]. A couple of quotes:

The situation is exacerbated by state and local election officials, whose primary concern is keeping election costs down and who put a premium on speed and convenience. As a result, 'the vendors don't particularly care about computer security because the marketplace doesn't care,' Greenhalgh insists." [Gary L. Greenhalgh, former director of the Federal Election Commissions' National Clearinghouse on Election Administration]

The piece quotes heavily from our very own PGN. My favorite:

`It takes trustworthy systems and trustworthy people to avoid tampering; it takes even more to avoid accidents from user operation or misuse,' Neumann says. `Our trusting of people and systems that are not trustworthy is an open invitation to disaster.'

[Thanks! PGN]

Re: Safety-critical software (Mellor, RISKS-15.19)

David Parnas <parnas@qusunt.eng.McMaster.CA> Fri, 5 Nov 1993 14:33:43 -0500

Pete Mellor wrote, "Prof. Cliff Jones of Manchester characterised the complexity of software in terms of the number of branch points it may contain, and hence the number of possible paths through it. The combinatorial explosion of possible paths makes exhaustive testing impossible in all but the simplest programs. It may be difficult to achieve with 50 Lines of code and 10 branch points. With 10,000 LOC and the same density of branch points, the testing time would exceed the time elapsed since the big bang. As he pointed out, the Sizewell B Primary Protection System contains 100,000 LOC."

It is worth remembering that were John von Neumann still alive, he might remind us that program state and data state are interchangeable, and that the number of sequences of data states in such programs is even larger than the number of sequences of control states. Even if we did test every possible path, we have not done exhaustive testing. We should not ever imply that such a test would be an exhaustive test.

Dave Parnas

✓ InterNet Mailing List

"JS McBride & Co. PostMaster" <jim_mcbride@netmail.com> Wed, 03 Nov 1993 09:56:28 pst

Here is the CORRECT info on the InterNet Mailing List.

Addresses are extracted from news feeds, list servers, and other sources. NO personal information is collected. The following is the ONLY information we collect.

- 1. Electronic mail address
- 2. User name
- 3. Search keywords
- 4. Date info was collected

The search keywords are limited to products.

Example: xwindows,unix,dos,ms-windows,emacs

To have your name removed from the list, send a message to DELETE@NETMAIL.COM Please place ANY addresses that you wanted removed from the list in the body of the message.

To get more info on how and why we are building the list, send a message to LISTINFO@NETMAIL.COM . [Just see next message. PGN]

Comments should be sent to TMANNING@NETMAIL.COM

Thank You, James McBride, NetMail, 415-949-4295

Auto Reply [What you get from LISTINFO. PGN]

"JS McBride & Co. PostMaster" <jim_mcbride@netmail.com> Wed, 03 Nov 1993 22:11:07

Thank you for your mail to Jim McBride at JS McBride & Company. Due to the volume of mail be handled by this account, this is an automatic reply.

PLEASE READ CAREFULLY!!

JS McBride is NOT collecting demographic information on email addresses.
 Due to the controversy surrounding this practice, we have discarded the product demographics we collected. We are however still collecting email addresses and user names.

- 2. The information collected (name and email address) will be offered in a printed white pages directory and in a white pages server on the net.
- 3. You DO NOT need to ask to have your name removed. BEFORE your name is used in the directory, you will receive mail asking for your permission. If you reply to the inquiry, your information will be used. If you do not reply, your name will NOT be used.
- 4. Comments regarding the white pages should be sent to Tom Manning at JS McBride & Company. <tmanning@netmail.com>
- 5. Mail to Jim McBride should be sent to <jimm@netmail.com>
- 6. Information regarding the purchase of the white pages directory should be sent to istinfo@netmail.com or telephone us at 415-949-4295

Thank you for your time, Jim McBride

Thanks to all of you (too many to note) who forwarded this to RISKS. PGN]

Security of the internet

<WHMurray@DOCKMASTER.NCSC.MIL> Thu, 4 Nov 93 06:50 EST

Our esteemed moderator complains as follows (aside, but in normal voice from a high pulpit):

>....which is that system and network security stinks in most >systems, particularly those on the Internet.

Not true, Peter. System security stinks on one system in five in the internet. This is not "most." However, it is sufficient to put the whole net at risk.

The level of security in the internet is. That is to say it is a given; the laws associated with large numbers make it resistant to change.

It is sufficient for most of the applications or uses of the net. Otherwise, by definition, the uses would not take place. At the same time it is insufficient for many of the applications.

Users of the net must understand that it is an "open" net. They may not rely upon the security of such a network. They may not rely upon the apparent origin or destination of the messages. They may not rely upon the behavior of privileged users (system managers et. al.) within the net. They not rely upon the polite behavior of users of the net.

This is not because the origin and destination of many messages are forged, that many privileged users are malicious, or that most users are rude. If

this were the case, the net would simply disintegrate. Rather, it is simply in the nature of an open network that some will be.

If it is important to your application that a message came from where it appears to have come from, then you had better have sufficient evidence, independent of that which the net provides you, that that is where it came from. If it is important to you that your message not be seen by anyone other than its addressee, you had better talk in a code that only you and he understand.

It is now relatively simple to automate such protection for your traffic at the application layer. Once automated its use will be simple and transparent. You will be able to enjoy both the wide connectivity and economy provided by the net and the security required for your application.

It is unrealistic to expect to get both, by default, from the same mechanism. The real world does not work that way.

William Hugh Murray, Executive Consultant, 49 Locust Avenue, Suite 104; New Canaan, Connecticut 06840 1-0-ATT-0-700-WMURRAY; WHMurray@DOCKMASTER.NCSC.MIL

★ Re: Security of the internet

RISKS Forum <risks@csl.sri.com> Fri, 5 Nov 93 16:40:18 PST

Bill, Consider the network as a system in the large. If almost all of those systems use passwords, their security stinks. [Only a few systems today use token authenticators.]

If a Trojan horse in my system captures a password on your system as a result of an FTP or TELNET from my system to yours, then YOUR system is now vulnerable to an attack that might permit me to Trojan horse your system, which in turn can compromise all of the systems that you FTP or TELNET to. It is as simple as that. By induction, virtually the entire net is at risk sooner or later, by iterative closure [cloture?].

Peter

✓ Yu, "Automated Proofs of Object Code..." available

<horning@src.dec.com>
Thu, 04 Nov 93 11:28:54 -0800

The following SRC Research Report is now available via FTP on gatekeeper.dec.com in: pub/DEC/SRC/research-reports/ or in hardcopy (send an e-mail request to src-report@src.dec.com)

This report is based on Yuan Yu's Ph.D. dissertation, supervised by Bob Boyer at the University of Texas at Austin.

"Automated Proofs of Object Code for a Widely Used Microprocessor", Yuan Yu, Report #114, October 5, 1993. 122 pages.

Computing devices can be specified and studied mathematically. Formal specification of computing devices has many advantages; it provides a precise characterization of the computational model, and allows for mathematical reasoning about models of the computing devices and programs executed on them. While there has been a large body of research on program proving, work has almost exclusively focused on programs written in high-level programming languages. Here we address the important but largely ignored problem of machine-code program proving. This work formally describes a substantial subset of the MC68020, a widely used microprocessor built by Motorola, within the mathematical logic of the automated reasoning system Ngthm a.k.a. the Boyer-Moore Theorem Proving System. Based on this formal model, we mechanized a mathematical theory to automate reasoning about object code programs. We then mechanically checked the correctness of MC68020 object code programs for binary search, Hoare's Quick Sort, the Berkeley Unix C string library, and other well-known algorithms. The object code for these examples was generated using the Gnu C, the Verdix Ada, and the AKCL Common Lisp compilers.

✓ "Research Directions in Database Security" ed. by Teresa Lunt

"Rob Slade, Ed. DECrypt & ComNet, VARUG rep" <roberts@decus.arc.ab.ca> 5 Nov 93 9:55 -0600

BKRDDBSC.RVW 931014

Springer-Verlag, 175 Fifth Ave., New York, NY 10010, 212-460-1500, 800-777-4643 or 8 Alexandra Road, London SW19 7JZ, UK 44-81-947 5885 "Research Directions in Database Security", Lunt (ed.), 1992, U\$39.50

Generally, we speak of security in binary terms. You either allow access to the system or you don't. You allow a file to be modified, or you don't. There are, of course, some very complex issues to be faced, and access situations can certainly become complicated. But by and large, access security can be resolved to a series of yes/no questions.

Not so with database security. The situation is almost the reverse of access security: there is no black or white, only shades of grey. In database security you have to assume that everyone needs and has access to the database, but that certain answers are not to be given to certain people. That's a fairly simple problem to deal with. What about the situation where many people can update but you don't want two people simultaneously updating the same record, and thus corrupting the data. Again, some reasonably simple solutions; although, when we add together many "simple" solutions, we start to build a fairly "complex" system.

Let's return to the question of access to information, using the example of the census data. There is no problem with anyone and everyone knowing how many people are unemployed in Canada. An aggregate number for British Columbia, or

even for North Vancouver, should still present no problems of confidentiality. However, no one should know that Robert M. Slade is unemployed unless Robert M. Slade chooses to divulge that datum. Even then, Robert M. Slade should have control over who should know that fact. Therefore, we have a situation where the individual records should not be divulged, but queries reported over a range can be. (Just to ensure that the issue doesn't get any easier, we have to build in safeguards that would prevent the indirect revelation of information such as generating queries of intersecting sets and watching the changes.)

Such are the questions addressed in this book. The contents are basically the results of a three-day symposium held in 1988. Sponsored by the military, many of the papers specifically address "classified" data, but a number of the concepts have practical business applications as well. (The military involvement may also explain the four-year lead time until the book was published.)

The book covers questions at all levels of the computing enterprise, from computer architecture through operating systems to data base architecture to conceptual approaches. Not all possible topics are covered, but there is a good range.

This is, quite definitely, for the database professional, and prior database security background would be helpful. The "alphabet soup," as Dorothy Denning notes, flies thick and fast. Most of the papers discuss TCB: the book is about finished before a paper tells you what it is (trusted computer base). The acronyms multiply, even using other acronyms: halfway through one paper on "A1 Secure DBMS (database management system) Architecture" the authors start talking about "ASD".

As with all such omnibus volumes, the interest will vary with the topic, and the quality varies with the author. One essay examines the "man in the loop" question in regard to the feasibility of automatic classification of data. After spending seven pages clarifying the question, the answer is basically, "No, computers can't understand text yet." Generally, however, the title is accurate. These are the "cutting edge" (or perhaps *slightly* behind) issues in data security, and an interesting discussion piece for those issues.

copyright Robert M. Slade, 1993 BKRDDBSC.RVW 931014
Permission granted to distribute with unedited copies of the Digest

DECUS Canada Communications, Desktop, Education and Security group newsletters Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733 DECUS Symposium '94, Vancouver, BC, Mar 1-3, 1994, contact: rulag@decus.ca

Re: CERT Reports and system breakins

Phil Karn <karn@qualcomm.com> Thu, 4 Nov 93 10:23:44 -0800

Ethernet addresses are *hardly* the basis of an effective authentication

scheme. On most controllers I know, the manufacturer-assigned Ethernet address is contained in a PROM, and the driver software must copy it to a register in the Ethernet controller itself. And nothing prevents the software from writing any address it likes, though of course in normal operation there is no reason not to.

I understand that IEEE 802.3 actually requires this capability (no doubt at DEC's behest since DECNET uses its own Ethernet addresses and ignores the PROM).

It would not be sufficient to argue that modifying the Ethernet address on "most" systems is "difficult" -- it's quite trivial to do it on many others, particularly PCs, for which networking hardware and software sources are readily available.

We need strong security mechanisms based on good cryptography and well thought out protocols. They're underway, but they will take time to develop. Although it's tempting to toss out little quick hacks that might complicate a cracker's life for, oh maybe 15 minutes or so, this sort of thing only diverts us from the effort required to provide meaningful security in the long run.

Phil

★ Re: CERT Reports and system breakins

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Thu, 4 Nov 93 13:35:32 -0500

Sorry, the original post was in haste and I am regretting that now - not that it was made but that I did not go into sufficient detail (and with the aid of 20-20 hindsight).

What I should have made clear is that if the hardware addresses are known for "approved" systems, then "unapproved" addresses will stand out and "unapproved" system could include the case of the router/bridge to the outside world.

Certainly it is possible to change a hardware address (though I had not realized just how easy it was) but that changer has a choice - picking another "unapproved" number really does no good while picking an "approved" number risks collision. Further if the hardware address is masked when it leaves my site, changing the number does no good.

So we are left with the case of and "approved" address that I can retrieve and now there are other checks possible once the "approved" system identification is known e.g. manufacturer, type of equipment, embedded system information. Still all spoofable but it now is getting to be a major undertaking that must start from the inside.

Add on the ability to retrieve which hub the contact is on and we are approaching the case that it is easier for the intruder to use the spoofed machine than it is to spoof it.

I thoroughly agree that effective encryption solves most authentication problems in one motion - just look at what I was writing in InfoSecurity News and a couple of other places over the last few years. The difference is that hardware address usage is simple, effective as a discriminant, and adds a layer of security that was not there before.

Padgett

Call for Participation - FIRST Incident Response Tools Work Grp

"Michael S. Hines" <MSHINES@freh-03ms.adpc.purdue.edu>
3 Nov 93 13:27:33 EST

***** * * * SECOND NOTICE * * * * * * * * *

The Incident Response Tools Working Group (IRTWG) of the Forum of Indicent Response and Security Teams (FIRST) has been formed for the purpose of developing a catalog to assist incident response teams (often called Computer Emergency Response Teams or CERTs) in the selection and acquisition of tools for use in incident response tasks. The catalogue will be available in electronic form to anyone who wants a copy.

David Curry of the Purdue CERT (PCERT) is chairing the group. My name is Mike Hines, also of the PCERT. I am a Senior Internal Auditor for Information Systems at Purdue. I have volunteered to coordinate compilation of a mailing list of potential providers of tools for use in incident response situations.

At this point I need two pieces of information from you:

- (1) An indication if you would like to assist me in compilation of this mailing list. We want to get as broad of coverage as is possible in this task. If you happen to have a source of several addresses, I would like your assistance. This is mostly providing me leads so we achieve as wide of coverage as is possible. I will be creating and maintaining the mailing list here at Purdue.
- (2) Any and all leads for sources of tools for incident response handling. Areas we are focusing on are:
- (a) Incident Detection... tools such as virus scanners, file integrity checkers, auditing systems, and intrusion detection systems... tools which monitor systems for signs of security violations.
- (b) Incident Response...tools such as keystroke monitoring systems, network packet capture, program disassemblers, and source code fingerprinting...tools which can be used to gather information during an incident.
- (c) Indicent Recovery...tools such as virus eradicators and file integrity checkers...tools which can be used to determine the scope of the damage done during an incident and which can help restore the sytem to pre-incident state.

(d) Incident Tracking...tools such as specialized database systems of one sort or another...tools which can be used to maintain statistics about incidents and archives of know attacks and defenses.

For each vendor/publisher/creator of tools in the above categories, please send the following information:

Contact Name:

Company Name:

Street Address:

City:

State:

Zip/Postal Code:

Country:

E-Mail Address of Contact:

Product Name(s):

Also if you know of another person who would be a good contact as a source of leads, please send their name and e-mail address along. I will contact them with this message to solicit new leads.

Thank you for your assistance.

Michael S. Hines, Internal Auditor-EDP, Purdue University, 1065 Freehafer Hall, West Lafayette, IN 47907-1065 mshines@ia.purdue.edu (317) 494-5845



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 23

Saturday 6 November 1993

Contents

Another plane lands on the taxiway

Lord Wodehouse

Pax Technologica? Not in Somalia

Peter Wayner

Teachers Beware!

Peter G Spera

Clerk stole from ATMs he was told to top up ...

Apte Kishor Hanamant

Notice of Fire Hazard with Dell Notebook Computers

Bob Robillard

"Eye of the Storm" (*another* Desert Storm virus?)

Rob Slade

Re: White House and STONED 3 virus

Andrew Klossner

Jon Grantham

Re: Ethernet addresses as "port" ids

Brian Bulkowski

Re: CERT Reports and system breakins

Allan Duncan

Re: Fiber Optic Cable Hazards

Gordon Mitchell

Re: "RSI does not exist"

Pete Mellor

Re: Magnetic Fields in Subway Cars

Bob Frankston

Kenneth R Foster

lan Turton

Peter Gorny

Bruce Limber

Russ Cage

Graeme Thomas

Info on RISKS (comp.risks)

Another plane lands on the taxiway

Lord Wodehouse <w0400@ggr.co.uk> Wed, 3 Nov 1993 10:24:37 +0000 (GMT)

In the most recent Flight International, there is an article about an Air Malta 737(?), which landed on the taxiway, instead of the runway. In summary the situation was as follows The airport has only one runway for normal use. The taxiway for this runway can be used as a runway, if the main one is closed. There is a normal sized taxiway as well.

The main runway was closed for maintenance, and the taxiway/runway lit as the runway as required. The small taxiway was lit as a taxiway. The Air Malta pilot was landing at night, saw the lit runway, and because he knew the main runway was closed, decided that he should land on the taxiway. Because of the repairs, the ILS system lined up with the main runway could not be used, so the pilot thought he was doing the right thing.

Exactly the same thing happened a year or two ago, when there was major work on the main runway. The only difference was that the direction of landing was reversed.

The moral here which applies in many other areas, including computers and their software is that people when they know that something has been changed and are presented with what appears to be the normal situation or choices, choose to take the alternative option, even when that is wrong. The pilot assuming that the lit runway was the one under maintenance chooses the taxiway, while the airport authorities assumed that by telling the pilots the runway was under maintenance and then lighting the runway/taxiway for use, thought this was correct. Perhaps they should a way of lighting the main runway in such a way that pilots can see that it is there, but obviously not in use.

Lord John - The Programming Peer, w0400@ggr.co.uk fax - +44 81 423 4070

Pax Technologica? Not in Somalia

Peter Wayner <pcw@access.digex.net> Fri, 5 Nov 1993 10:56:33 -0500

The reason why the NSA would like to stop crypto from being exported is because it could fall into the hands of US adversaries. People like General Aideed. But a recent story by Jack Anderson and Doug Cohn shows the danger of assuming that a technological advantage is is a guaranteed win. The article reads:

"[Aideed] had eyes and ears everywhere; he planted loyalists inside the UN headquarters itself; they kept Aideed informed of every move the Rangers made.

He had fun with them; he played embarrassing jokes on them. He fed them false intelligence, which sent them on wild goose chases. Once they raided a UN development project. They handcuffed and manhandled eight UN workers including four foreigners.

Another time, they descended on a compound, rounded up three dozen

Somalians and pushed around their leaders. The Rangers were told that Aideed was hiding out there. They grabbed a bald-headed man who looked like Aideed. When he denied it, they struck him with a rifle butt. So he hastily confessed that he was Aideed.

But he wasn't. He was security chief for Aideed's arch enemy, Ali Mahdi Mohamed, who was cooperating with the UN."

It is not clear how Aideed fed the Rangers the false intelligence, but it is conceivable that he just arranged for it to be broadcast in the clear.

In Chuck Yeager's biography, _Yeager_, the General made a point of telling of the time that he consistently beat someone in a dog fight ("waxed their fanny") despite the fact that he was flying a plane that was technologically inferior. It was the pilot, not the plane. Technology wasn't a surrogate for being clever.

Teachers Beware!

"Peter G Spera ((914) 296-6054)" <sperap@vnet.IBM.COM> Fri, 5 Nov 93 10:04:40 EST

First there was writing in the palm of the hand, then the crib sheet (or back of the tie or sole of the shoe or etc.), next came the programmable calculator, now coming to a store near you, the Newton generation.

The Newton Message Pad (Apple's new personal digital assistant) will have several financial and sophisticated calculator applications available to users. The hardware itself has 640 KB of storage for those hard to remember formula and definitions. There are also 1 and 2 MB storage cards available to expand the Message Pad's memory in preparation for midterms and finals.

If this is an acceptable risk for taking in-class tests, don't forget about the Message Pad's "Beaming" feature. The built-in infrared transceiver will allow 2 Newtons to exchange data up to 3 feet apart. This is particularly convenient when students want to split the preparation time or need a real time solution.

Clerk stole from ATMs he was told to top up ...

Apte Kishor Hanamant <kishor@iti.gov.sg> Wed, 3 Nov 1993 09:51:15 GMT

>From Straits Times (Singapore) dated 2 Nov 1993, page 21:

His job was to top up ATM machines with cash. Instead, he filled his own wallet - with \$122,000. Ahmed Ansar, a clerk with a security company filched \$ 250 to \$19, 350 on 22 different occasions between September 92 and September 93 from the ATMs at the Changi Airport. He was discovered and apprehended in a sting operation and confessed to his other crimes.

How is it that the fraud was not detected for over 12 months?

Does it not show a surprising and damaging lacuna in the whole system?

Would a manual cashier be allowed to run short for one year?

In another incident, reported in September of this year, a man was convicted of rigging a lottery run by a bank. He rigged the lottery to reward himself and his accomplices.

It appears that Singapore is racing towards computerization without devoting much thought to the risks and security issues involved.

Notice of Fire Hazard with Dell Notebook Computers

Bob Robillard <duke@iscp.bellcore.com> Tue, 2 Nov 1993 16:51:02 -0500

This has just been distributed at work; I thought I'd pass it on.

Talk about a hot machine....

Duke Robillard, duke@cc.bellcore.com

IMPORTANT SAFETY NOTICE concerning DELL 320SLi and 325SLi Notebook

Our records indicate you are the owner of a Dell 320SLi or 325 SLi notebook computer. We have recently discovered a potential fire hazard exists within your system. For your safety, you should discontinue use of the notebook immediately. Please also advise any other users of this system not to use it until repairs can be made.

Dell would like to repair your system free of charge and we ask that you return the system to Dell so we can repair it and return it to you as quickly as possible. To arrange for the repair, please call Dell at 1-800-847-4171 Monday through Friday between 8:00 a.m. and 6:00 p.m. Central Time. A special customer service representative will be ready to assist you and answer any questions you may have. Dell will send you a shipping box overnight and will arrange for next day delivery of your system to our repair facility. Please accept my apology for any inconvenience this may cause. Thank you.

Sincerely, John Medica, Vice President, Portable Products

"Eye of the Storm" (*another* Desert Storm virus?:-)

"Rob Slade, Ed. DECrypt & ComNet, VARUG rep" <roberts@decus.arc.ab.ca> 4 Nov 93 12:12 -0600

BKEYESTM.RVW 931019

Gold Eagle/Worldwide

225 Duncan Mill Road Don Mills, Ontario M3B 3K9 "Eye of the Storm"

Those who like books with series titles like "The Executioner" will like this book. 'Nuff said.

The computer virus is by no stretch of anyone's imagination a major subplot, even in a book which seems to consist only of subplots. Nevertheless, it is interesting to note what it indicates about the popular perception of viral programs.

The "virus" is tripped during an attempt to find a tap in a voice (phone and radio) network. Since phone switches are basically computers with special peripherals, this could be realistic. There are viral programs which can "sense" probes into memory or operations, and can then trigger. However, there is no indication of reproduction in the story, and, therefore, the malicious program is either a logic bomb or a trojan horse (or both).

Interestingly, the system under attack is protected by a "worm". The theory is proposed that you protect your own computer by shutting down if you detect suspicious activity. (One suspects this was the idea behind the "Immunizer".) Having written the shutdown program, you should know how to recover the system, whereas unknown malicious software can damage your data structure in ways that may take longer to diagnose and rectify.

The concept is initially interesting, but somewhat flawed. First of all, the reliability of the system is internally compromised by such protection, and this is not acceptable in all situations. (In the book, communications are shut down at a vital juncture.) Further, the detection of suspicious activity requires a background of known methods of attack. (Interestingly, the protection program in the book is stated to be subject to periodic upgrading.) Given the need for specific knowledge of security loopholes that the malicious software might use, there will probably be better means to deal with the insecurities. Finally, if the attacking program uses an unknown method, the attack may still succeed.

In the book, we once again see the myth of a virus (or the defending "worm" in this case) being able to damage hardware. Fuses blow, wires burn out and the power for the entire complex shuts down. Debugging the system involves the "MIS manager" character crawling under desks with a roll of electrical tape. Guess we still have some educating to do.

copyright Robert M. Slade, 1993 BKEYESTM.RVW 931019
Permission granted to distribute with unedited copies of the Digest

DECUS Canada Communications, Desktop, Education and Security group newsletters Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733 DECUS Symposium '94, Vancouver, BC, Mar 1-3, 1994, contact: rulag@decus.ca

★ Re: White House and STONED 3 virus

Andrew Klossner <andrew@frip.wv.tek.com> Tue, 2 Nov 93 12:51:28 PST

"Rush Limbaugh always uses whatever anti-Clinton story he can find, but only one recipient of the disk reported infection with the STONED 3 virus; the others had no infection, suggesting that it didn't originate at the White House."

Thanks. The report didn't quite ring true -- who boots from floopy these days? Perhaps the story is of more value in the statement it makes about uncritical social acceptance of computer RISK anecdotes.

-=- Andrew Klossner (andrew@frip.wv.tek.com)

Re: White House and STONED 3 virus

Jon Grantham <grantham@joe.math.uga.edu> Tue, 2 Nov 1993 19:27:13 -0500 (EST)

What actually happened, according to an AP article I read, was that one organization found the STONED 3 virus on the disk. Since they couldn't find any other potential source, they decided it *must* have come from the White House and not their own systems. They then put out an announcement to this effect, which was received with much joy by talk-show hosts. Neither AP nor the White House found anybody else who had the same problem, leading one to guess that the organization was wrong. The way the one disk became all of them is a topic better discussed in the alt.folklore hierarchy.

Jon

Ethernet addresses as "port" ids

Brian Bulkowski <bri>starlight.com>
Fri, 5 Nov 93 12:13:47 -0800

Various people have commented on the fact that Ethernet addresses can't be used for security because 1) Ethernet addresses don't get passed through routers, and 2) Ethernet addresses can be reset very easily. Some thoughts:

I caution against technology blinders. There are more network protocols than IP in the world. Microsoft's Netbios, for example, is inherently non-routable, so Ethernet addresses could be used for security. Novell's IPX uses the Ethernet address for the node number in the network layer address, which will be maintained across routers. Netware allows you to set a security list for a given user, and that user may only log in from certain Ethernet addresses in this fashion. I'm told the US government is a big fan of this feature.

In IP cloud land, it turns out that security on IP addresses is quite good, because any gross impersonation of an IP number will cause the return packets

to be routed someplace completely different.

The second is very true. They days of burning Ethernet addresses into real ROM is gone. Remember how big the form factor is for those things, and how long it takes to burn them? Most modern Ethernet cards that I'm aware of are software settable, which allows the manufacturer to set the ethernet address as part of the final software test of the board. This is far cheaper and faster than burning ROM. The 3Com ElinkIII, WD(SMC)16, Intel Etherexpress all do this, and come with a program to reset the Ethernet address. The risk is that that which is most flexible can be bent to nefarious purposes.

Regards, BrianB brianb@starlight.com

★ re: CERT Reports and system breakins (Peterson, RISKS-15.18)

Allan Duncan <a.duncan@trl.oz.au> Sat, 6 Nov 1993 22:33:14 +1100

- > ... It would be very
- > difficult (well, nothing is impossible but this would be close) for software
- > to forge an address using commercial equipment and collisions should be
- > obvious.

Well, that's the theory. I have an acquaintance who was working on a job with _lots_ of cards, and he found duplicate numbers. It made for an interesting bit of debugging until this was determined - you have to first over-ride the assumption that each device is unique.

Allan Duncan, Telecom Research Labs, PO Box 249, Clayton, Victoria, 3168, Australia. (+613) 253 6708 {uunet,hplabs,ukc}!munnari!trl.oz.au!a.duncan

✓ Re: Fiber Optic Cable Hazards

Gordon Mitchell <gordonlm@stein3.u.washington.edu> 3 Nov 1993 01:20:03 GMT

>I read with interest the story about the Telecom Worker who had died from >accidentally getting a piece of fiber into his bloodstream. Since I didn't >see much activity on this list about it, I sent out messages to a Telecom and >Safety list. [...]

>Anyone one else get any pertinent personal replies they can pass along?

I have worked with fibers for the last 20 years. Essentially since they became transparent. In that time I _have_ seen injuries of fiber stuck into hands. Fortunately silica is about as inert as materials come. The problem is generally more what is on the fiber, e.g., uncured epoxy.

The fiber in heart sounds like a scare story. As far as I am aware, the only hazard is mechanical irritation. That is pretty benign with hands. One occasional problem that occurs with buffer removed from fiber is glass flying

through the air when a fiber is bent and broken. That makes safety glasses a good idea.

Looking back over the last 2 decades, I can remember lots more wounds due to general lab hazards such as xacto knives, needles, hand tools,...

Gordon Mitchell gordonm@ee.washington.edu

★ Re: "RSI does not exist" (Gavin Matthews: RISKS Digest 15.21)

Pete Mellor <pm@csr.city.ac.uk> Wed, 3 Nov 93 00:42:19 GMT

Gavin Matthews <GAVIN@shapel.ug.eds.com> reported the ruling by Judge John Prosser, QC, in the case of Mughal versus Reuters.

This ruling has created uproar. It was front page news on most serious papers last Friday. The news is good for Reuters, who would otherwise face a series of hefty claims from its employees (or ex-, as in this case).

The good news for RSI sufferers is that the case will probably go to appeal, and the judgement stands a good chance of being reversed. (It seems to have been a test case backed by the NUJ.) Also, it does not constitute a "precedent" since earlier court judgements *have* awarded substantial damages to victims of this "imaginary" condition.

If you want to know how prevalent a condition is, ask yourself how many people you know personally are suffering from it. Since I became interested in the subject, I have discovered an amazing number of people who have.

My interest is personal. A close friend of mine was diagnosed as suffering from Carpal Tunnel Syndrome (CTS) a couple of years ago. CTS is a rather nasty form of RSI, and can lead to severe disability of the hands if not treated. It is due to the compression of the nerves in the wrist due to swelling of the surrounding tissues. My friend's case was typical. In retrosepct, she had suffered from it for many years, but the earlier diagnosis had been "arthritis". Following a fairly routine operation to relieve the pressure on the nerve, she has now made an almost complete recovery.

I put out a call for information on the net, and I was overwhelmed by the response. (This was *only* to do with CTS, not other forms of RSI.) Typists are not the only sufferers from CTS. Other professions/activities with a high incidence are: meat-packers, sheet-metal workers, pianists, cyclists, embroiderers, bricklayers. All involve repetitive actions with the wrist in a fairly fixed position. Predisposing factors seem to be: small frame (i.e., narrow Carpal Tunnel) and overweight. ("Egg-shell personality" didn't seem to be positively correlated! :-)

The use of word-processors, however, does seem to have coincided with an epidemic of CTS. The causes are a subject for speculation, but there are a number of interesting possibilities:-

- The use of a computer terminal involves long periods of keying without changing hand position (as opposed to the old manual machines which required the typist to change paper occasionally).
- The condition is far more prevalent than was realised in the past, and was under-reported due to misdiagnosis. (CTS has only recently become a recognised condition: see my friend's previous diagnosis. Also, a number of the people who responded to my request for information cited cases of parents or other older relatives who ended up almost totally crippled with what was obviously CTS, but could not be diagnosed or treated at the time.)

However, thanks to Prosser's judgement, we can all relax. My friend can rest assured that her symptoms were "all in the mind", including the wasted muscles on the affected hand, and the appearance of the nerve when exposed. (This was obviously an interesting case of "mind over matter": the thought compresses the nerve! :-) Her recovery must be an interesting example of the "placebo effect".

Reuters can get away without paying their disabled employees a penny (for the time being! :-) and the surgeon who operated on my friend's wrist can cut down his operating list (*one* surgeon in *one* clinic dealing with 4 or 5 cases *each week*!) by referring all his patients to a psychiatrist! :-)

Anyway, typing all this has made my hand feel a bit funny. (Must be my "egg-shell personality"!) I think I'll give it a rest.

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB Tel: +44 (71) 477-8422 p.mellor@csr.city.ac.uk

Disclaimer: British justice is a fine institution. Neither I nor my employers would ever dream of suggesting that a distinguished judge could be senile, corrupt, or both.

★ Re: Magnetic Fields in Subway Cars (Drzyzgula RISKS-15.20)

<Bob_Frankston@frankston.com> Tue, 2 Nov 1993 19:30 -0400

The obvious question: "What about Maglev systems". They use very strong magnetic fields to propel the train.

magnetic fields on subways

Kenneth R Foster <kfoster@eniac.seas.upenn.edu> Tue, 2 Nov 93 19:35:01 -0500

I've been a consultant, in an indirect way, to a Department of Transportation study of magnetic fields on trains, and have analyzed data from several railroad systems (French TGV, Boston subway system, Northeast Corridor AMTRAK system in the US, Washington Metro). The fields can be quite high -- several Gauss near the floor. The frequency content depends on whether the system

operates at AC or DC. The fields are associated with motors running the trains, the catenaries, etc. I do not know what kinds of fields are needed to wipe out floppy disks but there is a wealth of data on magnetic field dosimetry available.

I note that the fields are strongest near the floor of the cars and near motors. At seat level they are generally comparable to other ambient fields. Maybe dropping the disk on the floor near a motor would be the most likely source of trouble.

Kenneth R. Foster, Bioengineering, Univ. of PA

★ Re: Magnetic Fields in the subway (Marchant-Shapiro, RISKS-15.21)

Ian Turton <ian@geog.leeds.ac.uk> Wed, 3 Nov 93 09:08:09 GMT

Several years ago I was a student at the department of geophysics in Newcastle upon Tyne. One story told to us was that shortly after the city opened its metro system, one line of which ran past the university, the department started to have problems with its magnetometers, which measure changes in the Earth's magnetic field on the order of 1%. It turned out that the safety cutouts to earth on the metro system where underrated by a factor of 10 and hence most of the current was flowing to ground instead of back along the tracks, the system uses overhead cables to carry the positive supply. This meant that there was no opposing magnetic field from the rails to cancel the overhead cable's field. The department actually had a contract for a while to report to the City where the circuit breakers had blown, which they could tell by triangulating the pulses of magnetism.

So it seems possible that the designers of the DC metro didn't consider the size of magnetic fields generated by the system and didn't use a specific return path or that they have a problem with this path anyway.

On a related note the fears of the London Underground lead to BBC radio personel always travelling by taxi when carrying magnetic tapes, though I never heard of anyone actually having a magnetic tape damaged on the underground. However the expenses are better on a taxi :-)

Ian Turton - School of Geography, Leeds University, Leeds, UK. 0532 -333309

★ Re: Magnetic Fields in Subway Cars (Drzyzgula, RISKS-15.20)

Peter Gorny <Peter.Gorny@arbi.informatik.uni-oldenburg.de> Wed, 3 Nov 1993 18:46:26 GMT

Well, I lost all data on a 1/2" magnetic tape that way in a Hamburg streetcar many years ago. (To recover I had to travel 200 miles back to the source computer.... so I know what you are talking about.

BTW: Beware of loudspeakers. They often have strong permanent magnets.

D-26111 Oldenburg, Germany +49-441-798-2901 or -4521 (Fax: -2155) Gorny@Informatik.Uni-Oldenburg.DE Gorny@ACM.org

Re: Magnetic fields on subway trains (and elsewhere!)

Bruce Limber <bli>blimber@cap.gwu.edu>
Wed, 3 Nov 1993 13:56:27 -0500 (EST)

There's lately been discussion here of the possible RISKS to magnetic media of the magnetic fields in subway trains. As a regular commuter on Washington, DC's Metro, I find this a subject of considerable interest.

(And while I've been known to carry floppy disks and/or a laptop computer on the trains, no, I haven't noticed a problem so far.)

That said, can someone out there with the appropriate expertise please advise the rest of us, whose fields are regrettably not sufficiently broad that we can figure out the answer for ourselves?

Is there a way to transport magnetic media safely, so that they're protected from errant fields on subways and elsewhere? If so, how?

- In closed ferrous boxes?
- Closed non-ferrous boxes?
- Sprinkled with the blood of a freshly-killed goat?
- "Grounding" the box, or not?

Inquiring minds want to know. . .

(BTW, I've also heard it said that we need not fear airport X-ray machines, but that library stolen-book detector gates are sudden death to disks. True, or not? I--for one--don't know.)

Re: Magnetic fields in subway cars (Drzyzgula, RISKS-15.20)

<rsi!russ@destroyer.rs.itd.umich.edu>
Thu, 4 Nov 93 23:13:41 -0500

I can vouch for Bob Drzyzgula's experience, from direct measurement. In 1989, I was working for one of the Big 3 auto companies developing an advanced electronic compass system. One of its features allowed continuous real-time readings of its flux-gate sensor. We used this to log hours of data to disk for later analysis. Typical data from a run would show the local magnetic field to be about 15-20 A/D counts (the sensitivity was about .02-.025 gauss/count; it was never measured exactly).

Our summer intern took a test car to NYC as part of a system shake-down. He happened to be logging data as he drove down 5th Avenue (if I recall correctly) and a train just happened to pass underneath. The magnetometer showed a deviation of several HUNDRED A/D counts off to the right of the

vehicle, followed by a return to normal a few seconds later. This was on the road above, mind you, not just a few feet from the rail. I would estimate the street-level field strength at 5-10 gauss.

One wonders how the inductive currents affect bone development in subway commuters, among other things. If magnetic fields affect other biological processes, it would appear that the subways are a health concern for anyone living next to a line. (Perhaps one could take a medical deduction for a penthouse dwelling?)

Russ Cage (313) 662-9259 russ%rsi.uucp@destroyer.rs.itd.umich.edu russ@m-net.ann-arbor.mi.us

Re: Magnetic Fields in Subway Cars

Graeme Thomas <gvt@uplx.co.uk> Sat, 6 Nov 93 12:37:07 GMT

I vaguely recall reading that the BBC used to have a rule preventing couriers carrying video tapes from travelling on the London Underground system, for fear that the magnetic fields would wipe the tapes. Instead, the couriers would use taxis, at greater expense. Eventually some research was done, which proved that the magnetic fields experienced inside the metal carrying cases was negligible, and the rule was eventually removed.

Graeme [gvt@uniplex.co.uk]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 24

Tuesday 9 November 1993

Contents

Smart Houses? No Thanks!

Jim Brown

Ada. a standard no more?

Luis Fernandes

Pets & data communication

Bruce Clement

Orange County DACS outage

Matt Holdrege

Review of Bruce Sterling's Hacker Crackdown

Peter B Ladkin

Alvin and Heidi Toffler's War and Anti-War

Jeffrey D. Young

Re: Car owners confused with gun owners

Martin Minow

Software control problems in Block 40 F-16s

Peter B Ladkin

Investment program turns into doomsday machine

Rogier Wolff

Re: Notice of Fire Hazard with Dell Notebook Computers

Don Porges

Internet Security

William Hugh Murray

Stupid language games

Richard Schroeppel

Networking on the Network

Richard Schroeppel

Anonymous postings

anonymous? No

Daniel Lieber

Properties of Anonymizing Service

Anthony E. Siegman

Risk-happy drivers foil anti-lock brakes

Dyane Bruce

Info on RISKS (comp.risks)

Smart Houses? No Thanks!

Jim Brown <jbrown@umi.com> Tue, 9 Nov 1993 14:04:18

While listening to a recent Marketplace Radio spot on Smart Houses I became, at first amused, then alarmed, by what is now possible with smart houses. (A smart house has an electronic control center that can be operated locally or remotely.) Access to the smart house control center is though an ID/PIN setup.

The amusing features (to me anyway) are having the 'house voice' reply to simple questions.

Alarming features were setting lighting, temperature, and other security features - even remotely over the phone! I can't think of something more intimidating that having some hacker/cracker take control of the electronic controls of my house!

What are these designers thinking who make these houses? Do they assume that an ID/PID setup is secure enough? And why on earth do they allow remote access via telephone- a very non-secure medium?

No smart house for me.

Jim Brown, 300 N. Zeeb Rd. Ann Arbor, MI 48106 (USA) (313) 761-4700 x3227 jbrown@umi.com

Ada, a standard no more?

luis fernandes <elf@ee.ryerson.ca> Sun, 7 Nov 93 11:54:33 EST

>From the October 11, 1993 issue of "Aviation Week & Space Technology":

The use of Ada as the standard Defense Dept. computer language should be rethought, the head of the Air Force Electronic System Center told an audience recently. "The Defence Department lost power years ago on computer development, but some don't realize it", Lt. General Gordon E. Fornell told the Society of Experimental Test Pilots. Instead of insisting on Ada, the best software for the task would be used-- and that software should be commercially available. "There are great dollar values out there", Fornell said. "It's obviously time for a little rethinking about Ada, and it's getting to the 'just do it' point".

✓ Pets & data communication

Bruce Clement <frey@alfheim.actrix.gen.nz> Mon Nov 08 16:32:24 1993 This happened tonight while I was reading RISKS.

I noticed that the lights on my modem were behaving strangely & switched the uucico program to the foreground. It was reporting a string of "NO DIALTONE" responses.

Picking up the study's phone, I found it to be dead. The extension in the lounge was also dead.

In a corner of the bedroom, I have the basestation for my Panasonic cordless phone (which can also act as a speaker phone) which was off hook, and presumably had been off hook long enough for the exchange to "notice".

As I had used the study's phone since arriving home, how this extension could be "off hook" was a mystery, which was not solved until I walked over to it & discovered /dev/pet (my rat) hiding behind the phone.

Why is the on/off button on a phone sufficiently sensitive to be tripped by 310 gramme rat walking over it?

Oh, yes, what's the risk? If I hadn't diagnosed the problem, UseNet wouldn't have been able to get to the computer, and as I wouldn't have been able to phone for pizza, the rat would have had to eat lab block again :-)

Bruce Clement (frey@alfheim.actrix.gen.nz)

✓ Orange County DACS outage

Urban Surfer <HOLDREGE@DCV4KD.PHS.COM> Tue, 09 Nov 1993 14:38:41 -0800 (PST)

About 6 weeks ago, I posted in the Telecom Digest an account of the DACS outage in Orange County, CA. I received several queries for more information. It seems that a lot of people were disturbed to learn about the potential points of failure on a DACS as well as the bug we experienced.

I recently took a tour of the affected CO and met with the switch and DACS administrators to ask further questions. At this point, they believe that they have fully addressed all software & procedural issues with the DACS IV. They also stated that the software patches they applied have been propagated throughout the entire Bell network.

Pac Bell, as required by law, filed a report of the outage to the FCC. This is a public document. I'm not sure what the normal method is for obtaining that document, but I know there is one. For those who need to know now, I received a copy by fax, retyped it put it up for anonymous FTP on DCV4KD.PHS.COM under DACS.OUTAGE.

Matt Holdrege matt@phs.com MH235

✓ Interesting book review --- Bruce Sterling's Hacker Crackdown

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 9 Nov 93 00:03:13 GMT (Tue)

The adjective may be chosen to modify either. Ian Stewart is a mathematician who writes wonderfully well, as readers may see by looking at his review, in the London Review of Books 15 (21) of 4 November 1993, of Bruce Sterling's `The Hacker Crackdown: Law and Disorder on the Electronic Frontier', Eric Raymond's edition of `The New Hacker's Dictionary', and Bryan Clough and Paul Mungo's `Approaching Zero, Data Crime and the Computer Underworld'. (I had wondered what Clough had been doing since he retired from soccer).

Stewart refers to various incidents, such as the 15 Jan 1990 4ESS problems, the stoned virus, the Internet worm (but when will people stop deprecating Eric by implication?), and the Secret Service crackdown on Steve Jackson games and `Knight Lightning'. Stewart's closing sentence: `"Approaching Zero" shows that we have a lot to fear from the activities of those (few) hackers who are genuinely malevolent. "The Hacker Crackdown" suggests that we have just as much to fear from programming errors - and that American citizens have far more to fear from their Secret Service.'

Peter Ladkin

✓ War and Anti-War (by Alvin and Heidi Toffler)

"Jeffrey D. Young" <0004784090@mcimail.com> Sun, 7 Nov 93 20:18 EST

>From the authors of "Future Shock" (1970), "The Third Wave" (1980), and "Power Shift" (1990), "War and Anti-War" (1993) looks at the way we make war and peace now and in the 21st century.

The Tofflers propose that as we move from an industrial society to an information society, changes in the way we make wealth will be reflected by changes in the way we make war (and hopefully peace).

Many of the concerns noted by Winn Schwartau in "Terminal Compromise" are echoed in "War and Anti-War", as well as some new concerns with more dire consequences.

War and Anti-War: Survival at the Dawn of the 21st Century by Alvin and Heidi Toffler Little, Brown and Company 1993 ISBN 0-316-85024-1

re: Car owners confused with gun owners (Hawthorne, RISKS-15.22)

Martin Minow <minow@apple.com> Tue, 9 Nov 93 10:43:42 -0800 Brian Hawthorne's description of a problem his wife had when she received a request to renew her firearm license because "someone loaded a tape containing the list of car owners who needed to renew their automobile registration instead of the list of gun owners needing to renew their carry permits" reminded me of a made for ty movie that was shown in Sweden in the mid-1970's.

Its premise was that the government computer that processed driving licenses was also processing hunting licenses [timesharing] and, because of "thought transference" between the two programs, the civil status of one Holger Swensson was changed from "married" to "elk."

Well, this was a problem, but one without a simple solution. Unfortunately, the local social welfare department cannot help elks. The situation became worse as time went on and hunting season quickly approached. Finally, a sympathetic bureaucrat hit upon the best solution: he found the one place where Holger would be safe and, in the last scene, you saw him spread his sleeping bag out in the Stockholm Zoo.

Kafka and Ionesco would have enjoyed this. [and made Rhinockwurst? PGN]

Martin Minow minow@apple.com

Software control problems in Block 40 F-16s

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
7 Nov 93 18:02:31 GMT (Sun)

Here is an example of a problem which has been partly attributed to software control of fly-by-wire aircraft. With aircraft, many factors usually contribute to a problem or an accident. That is, many factors are usually jointly necessary for a problem to occur, and no factor is itself sufficient. So partial attribution is the highest grade of causal involvement that one should normally expect.

Block-40 F-16's with the heavier wing-tip mounted AMRAAM AIM-120A's can endure 2g, 4-5Hz oscillations at the wingtips which caused problems severe enough (e.g. instruments could not be read in the cockpit) that a 550kt speed limit (TAS or IAS not stated) was imposed. This is to be lifted, since a fix has been found.

`Lockheed is developing new digital flight-control software for Block 40 F-16s. Use of the software will end restrictions which limit the aircraft to 550kt (1,000 km/h) when armed with [the AIM 120A's]. [....]' (Flight International, 3-9 Nov,p18).

'Investigation work by the test team has revealed that oscillations of between 4-5Hz, induced by the missile at the wing tip, are exacerbated by the flight control system, which effectively over-reacts to inputs from the aircraft's rate gyros. The USAF is evaluating modifications to the flight-control laws...' (Flight International, 20-26 Oct, p21).

`The test team believes that the phenomenon can be traced to the larger size

and weight of the AIM-120A, combined with the improved, four-channel digital flight control system, as well as structural differences of the heavier Block 40 aircraft.' (Flight International, 3-9-Nov, p18).

This latter article interviewed Lt. Col. John Armor, one of the test pilots 'working on the program'. So, we can assume this is an 'official' attribution of cause that includes the flight control system (whether software or hardware seems to me to matter less - it's the specification and the computational behavior that are under question), since it came direct from a member of the USAF.

Peter Ladkin

✓ Investment program turns into doomsday machine (v.d. Meulen, -15.21)

Rogier Wolff <wolff@liberator.et.tudelft.nl> Mon, 8 Nov 1993 18:14:41 +0100 (MET)

As a (very small scale) stockholder I'd like to make a few observations, corrections and additions.

- > The investment fund Groeigarant put the "Black Box" out of order. It was
- > designed by Ton Jongbloed, former president of Staal Bankiers, to advise
- > investors. He claimed on long term it would be twice as profitable as
- > investing in public loans. However the expert system EIS (Electronic
- > Investment Sector) proved to be a "doomsday machine". Only by disconnecting
- > it from the mains larger damage could be averted.

The system was never wired directly into the stockmarket. There has always been a sanity check of the programs output.

- > Roughly, the principle of the program was: buy when prices go down, sell > when prices go up.
- The principle is based on the assumption that a stockmarket price is an actual value, plus some added noise. They want to buy when <noise> is less than zero, and they want to sell when the <noise> value is larger than zero.

The program EIS works by calculating an estimate of the "actual value", and based on that it will know an estimate of the <noise> .

- > Therefore, EIS issued orders to sell only. It sold almost all
- > the stocks Groeigarant had, and would have sold even more. The latter would
- > have led to a very risky situation. Selling stocks not available can lead
- > to severe losses when forced to deliver (and having to buy at even higher
- > prices).

Contrary to other investment funds, Groeigarant changes rapidly between having 90+ % of the capital in stocks to having less than 10% in stocks.

Contrary to their original aim ("Groeigarant is a fund that will invest

in stocks available at the Dutch stock exchange"), they currently also invest at the options exchange.

- > Groeigarant says it will base its future investments on fundamental and
- > technical analysis of the stock market. Luckily, the consequences for the
- > fund have been kept to a minimum. Severe losses have been prevented. At the
- > moment the fund mainly possesses money, rather than stocks.

I have noticed that over the last two years, the "sanity check" went from "sanity check" to "this is what we want the system to say, so that's what we'll make it say". They have been "forcing the system to say what they want" for about a year now.

Another interesting thing: Since a few months they allow you to buy stock at the -*lowest*- price over a month (in hindsight :-)! Stock bought in this way can be sold again at the -*highest*- price. I could start this scam: I give them \$1000 every month, and sell the equivalent amount of stock each month. This gives me a sure strategy to make money: Groeigarant stockprices go up and down enormously. They do make money on the transaction costs, but these are very likely to be less than the difference between highest and lowest value over a months time.

The "management fee" that Groeigarant pays to the executives is interesting too: They calculate their return on investment (r.o.i) over a period of three months, subtract the r.o.i of the public loans and pay 25% of the result to the management. The funny thing is that even if the long-term return on investment is zero, the r.o.i. over a "small" period as three months can be higher, and they will pay. However there is no "reverse" rule, that goes into effect when the next three months the net result is negative.

I have this theory, that the decision to buy or to sell can be made on the basis of the ratio between todays and yesterdays price. However the transformation function is fractal, and can only be determined by inspecting actual data. I therefore train the computer based on the stockmarket prices of the last few years. Next, if I feed the computer the same data that it was fed in the learning phase, it will perfectly predict when to sell, and when to buy stock. This only happens on the dataset that it was trained with. On any other dataset, it will more or less generate random buy and sell advices, and incurr transaction costs.

This is more or less the effect what I have been suspecting in EIS since the beginning. Groeigarant denies that this is the case, and even claims that they didn't have the dataset: When they started they claimed enormous net results, that had been obtained on the last few years, but since the introduction (At least 3 years ago) they have exactly the same value right now as at the introduction.

Roger.

★ Re: Fire Hazard with Dell Notebook Computers (Robillard, RISKS-15.23)

Don Porges <porges@banshee.camb.inmet.com> Tue, 9 Nov 93 18:59:46 EST > ... Dell will send you a shipping box overnight and will arrange for > next day delivery of your system to our repair facility.

Assuming, that is, that 1-800-847-4171 really *is* Dell, and not a large-scale computer thief. Risks upon risks.

✓ Internet Security (PGN, RISKS-15.23)

William Hugh Murray <75126.1722@compuserve.com> 08 Nov 93 09:15:58 EST

>... By induction, virtually the entire net is at risk >sooner or later, by iterative closure [cloture?].

Beautifully and briefly argued. I agree completely and have so argued (see the Risks archives.)

The bad news is that we are adding new target nodes to the network at a much faster rate than we are protecting with token-based one-time passwords. The situation is getting worse not better. If I wait until the good behavior of my neighbors reduces the risk of the net, I will wait a very long time.

The good news is that I need not wait. I can remove my system from the target population for pennies per user per day. I can continue to enjoy the connectivity and economy of the net without the risk. I can do it unilaterally at the network, or even the computer, application layer.

Connectivity, lowest price, security; pick any two.

William Hugh Murray, Executive Consultant, 49 Locust Avenue, Suite 104; New Canaan, Connecticut 06840 1-0-ATT-0-700-WMURRAY; WHMurray@DOCKMASTER.NCSC.MIL

Stupid language games (Parnas, RISKS-15.22)

"Richard Schroeppel" <rcs@cs.arizona.edu> Sun, 7 Nov 1993 17:28:11 MST

Dave Parnas writes

Pete Mellor wrote, "Prof. Cliff Jones of Manchester characterised the complexity of software in terms of the number of branch points ...

Some peevish nits --

The first sentence of the Cliff Jones quote suggests that the number of paths through a piece of software is equal to, or perhaps proportional to, the number of branch points. Subsequent sentences correct this impression, but there must be a better way to state the relationship.

Nit2: The actual ratio of branch points to lines of code in my programs, and I suspect all readers of this message, is much less than 1/5, if function calls

are excluded; and higher than 1/1, if function calls are included.

Nit3: There's an implicit assumption in the Jones statement that the number of paths through the code is roughly exponential in the number of branch points. This depends entirely on the code, and need not be true: If I'm comparing two programs which generate reports, and one has 10000 lines and the other 100000 lines, it's perfectly possible that the larger program will require only ten times as much testing. The important questions are things like nesting depth, interlinked flow of control, interrupt handling, etc. Mere size is a weak indicator.

Nit4: I can't tell without more context, but are any of Jones, Mellor, or Parnas endorsing the position that only exhaustive testing is appropriate?

Nit5: What are we to mean by "exhaustive", anyway? If I have a 32bit computer, I can't even test the ADD instruction exhaustively, much less a program. [2^32 * 2^32 * 1 nsec = 600 years.] Let's talk about my carburetor:

It is worth remembering that were Gottlieb Wilhelm Daimler still alive, he might remind us that the composition of the gasoline (petrol) is important. If we consider the number of possible different mixtures of hexane, heptane, and octane, and their isomers, we can't possibly conduct an exhaustive test. Noone should ever imply that a carburetor has been exhaustively tested.

Can we please consider specific criticisms, rather than simply chanting "Big Is Ugly"?

Rich Schroeppel rcs@cs.arizona.edu

NETWORKING ON THE NETWORK

"Richard Schroeppel" <rcs@cs.arizona.edu> Sun, 7 Nov 1993 17:54:39 MST

Phil Agre recently offered us advice on how to network for success. I didn't see any response to his message, so I thought I'd offer a different view. I wish to go on record as stating

"I do not choose my friends based on their potential usefulness to my professional advancement. Even a little bit."

Rich Schroeppel rcs@cs.arizona.edu

Anonymous postings

<anonymous.poster@someplace.on.earth.l.think>
Mon, 8 Nov 93 13:17:34 -0800

This is in response to the dangers of anonymous postings as stated in RISKS-15.19. It is an interesting topic, but the idea of using a redirector

for anonymous postings is not required. As this message demonstrates (from anonymous.poster@someplace.on.earth.I.think), it is very easy to send anonymous mail from locations without a trace. (The possibility of it being traced is there, but not likely.) In fact, this particular message is being routed courtesy of the recipient's machine (PGN- please verify). I will not disclose this method of anonymous mailings to requesters -- it is public information. I wish you all the best of luck in your security issues. And now for who I am... --Daniel Lieber, Systems Manager, _The Vanguard_ at Bentley College, Waltham, Mass. USA <LIEBER_DANI@ Bentley.edu>.

Properties of Anonymizing Service

"Anthony E. Siegman" <siegman@sierra.stanford.edu> Sun, 7 Nov 93 19:54:39 PST

I was surprised to learn recently that if one replies to a message or newsgroup posting which has been anonymized by passing through the anon.penet.fi service, not only is your reply transmitted through to the original anonymous sender, but also you are assigned an anonymous code name and the connection between this code name and your real address is stored, presumably indefinitely, in the anonymizing service's files. You're not asked if you want this to happen, though you are informed it's been done.

I have no clearly formulated objections to anonymizing services like this -- though they clearly cause certain problems -- but I'm not sure I like this policy. A user who deliberately sends a message or newsgroup posting through such a service presumably agrees to its rules. But an individual who replies to such a message or posting may not have any idea what " anon.penet.fi" really is -- in fact, someone replying to a newsgroup posting may not even note what machine it came from -- and may not want to be added to their records.

To cite just one (perhaps far-fetched) risk, an anonymizing service might be used by bad guys to do some bad thing, causing law enforcement people to swoop in and seize records. Your name could then be found in those records, perhaps not clearly identified as a mere innocent "replier" rather than a deliberate user, leading to possible embarrassment or maybe worse.

The proprietor of the anon.penet.fi service has not yet replied to my inquiries concerning this policy. --AES

Risk-happy drivers foil anti-lock brakes

Dyane Bruce <db@diana.ocunix.on.ca> Sun, 7 Nov 1993 11:39:44 -0500

>From the Ottawa Citizen Sunday Edition November 7, 1993 Risk-happy drivers foil anti-lock brakes by Brad Evenson, Citizen consumer writer

Anti-lock brakes, hailed by car companies as a leap forward in auto

safety, do not reduce the number of accidents, injuries or deaths on the road, says a U.S. research group. And a recent Transport Canada study may have unlocked the reason why: people like risk.

Anti-lock brakes, standard equipment on a third of new vehicles sold in Canada, are designed to help drivers keep control on slippery roads. When a braking wheel loses traction, a sensor causes the brake to release and tighten rapidly many times, maintaining a grip on the road.

Technically, the systems perform well. But they've yield no change in accident statistics.

"The number of accidents, injuries and deaths has remained constant in models with ABS in the United States," says Brian O'Neill, head of the U.S. Insurance Institute for Highway Safety.

The group compared automobiles equipped with anti-lock brakes with the same models produced in the previous year that didn't have them. There was no appreciable difference, says O'Neill.

The Canadian experience is similar. In 1991, there were roughly 173,000 collisions involving 248,600 injuries and 3,684 deaths. Statistics for 1992, to be released this week, are expected to show a five-percent decline in accidents, but federal officials do not attribute the drop to anti-lock brakes.

The RCMP is one of the country's largest auto buyers, but there has not been any reduction in damage to its 7,000-vehicle fleet since ABS-equipped models were introduced three years ago. About a third of its vehicles now have the brake systems.

"In test, police drivers found they were able to manoeuvre more quickly," said RCMP spokesman Const. Tim Cogan. "But we haven't seen a difference in the number of accidents."

This has baffled car manufacturers such as General Motors, which advertises anti-lock brakes as a safety feature -- a crash-avoidance system preferable to air bags.

But a recent Canadian study offers an answer. At a test track in Blainville, Que., Transport Canada scientists divided 80 drivers into groups, testing their performance with anti-lock and ordinary brakes.

"After having practised the emergency stopping manoeuvres with antilock brakes, drivers drove faster, had higher accelerations around a curve and stopped harder," a summary of the study said.

"If drivers choose to drive faster because they know they have greater control, and if they choose to follow other vehicles more closely under slippery road conditions, then the safety benefit from anti-lock brakes might be reduced or lost completely."

The theory explaining the results is called "risk homeostasis," and it also explains why people bungee jump or helicopter ski.

"People like to maintain a constant level of risk," says Chris Wilson, director-general of road safety at Transport Canada.

"When a situation gets safer, people like to increase the level of risk."

Some authorities, however, scoff at the risk homeostasis theory. In the 1980s, GM sent a Detroit engineer to Canada to study whether drivers who wore seat belts drove recklessly "because they wouldn't get hurt in an accident," recalls Wilson of Transport Canada.

The engineer took photographs of drivers along Hwy. 401 [A major highway that runs through Toronto Ont. Canada db], checking seatbelt use against their driving habits.

He found no evidence of the theory; people drove the same with seat

belts on.

While the evidence of improved safety with anti-lock brakes is scanty, the life-saving record of airbags, which inflate upon collision, is more abundant.

"There is clear-cut, statistical proof the airbags improve your chances (of survival) in a collision," says the insurance institute's O'Neill

But car makers have resisted introducing airbags, complaining they are too expensive and don't help avoid accidents.

"An accident avoidance system (such as anti-lock brakes) is obviously better than one that doesn't prevent accidents," says Chris Douglas, product spokesman for GM of Canada Ltd.

Dyane Bruce, 29 Vanson Ave. Nepean On, K2E 6A9, 613-225-9920 db@diana.ocunix.on.ca



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 25

Weds 10 November 1993

Contents

No change in Ada policy

Robert I. Eachus

Groundhog Day, D-Day, Remembrance Day, and all that

Mark Brader

Not so easy to be anonymous

Robert L Ullmann

Snakes of Medusa and Cyberspace: Internet identity subversion

L. Detweiler

Info on RISKS (comp.risks)

No change in Ada policy

"Robert I. Eachus" <eachus@spectre.mitre.org> Wed, 10 Nov 1993 11:58:58 -0500

elf@ee.ryerson.ca (luis fernandes) quotes AvLeak:

- > The use of Ada as the standard Defense Dept. computer language
- > should be rethought, the head of the Air Force Electronic System
- > Center told an audience recently. "The Defence Department lost power
- > years ago on computer development, but some don't realize it", Lt.
- > General Gordon E. Fornell told the Society of Experimental Test
- > Pilots.

I don't see a direct connection to computer risks in that posting, other than the speed of propagation of information, whether true or misleading. In any case:

The new Ada standard (Ada 9X) is out for ballot, both in ANSI and ISO. The mechanics of the situation insure another ballot next year, but the right time for substantive comments is now.

The new Ada standard includes a Safety and Security Annex, Annex L, as well as other changes to reduce risks. Many readers of this group may want to

check this out.

Emmett Paige, Assistant Secretary of Defense for Command, Control, Communications and Intelligence recently said that his support for Ada was unwaivering. :-)

However, the new Ada standard does mean that the DoD policies WILL change to recognize the existence of the new standard. The current plan is that no program using Ada will be forced to transition to Ada 9X. But given the improvements in the language and the high degree of upward compatibility most programs are expected to switch relatively quickly.

Finally--and totally unrelated, other than the article as quoted is misleading--Lt. General Fornell retired on October 29th, after five years as head of Electronic Systems Center.

Robert I. Eachus

Groundhog Day, D-Day, Remembrance Day, and all that

<msb@sq.com>
Tue, 9 Nov 1993 22:00:31 -0500

A few days ago, in alt.folklore.computers, Michael Shapiro (mshapiro@netlink.nix.com) wrote:

I do have one debugging rule, learned the day after a test of some date dependent software. "Never test date-dependent software on February 2, March 3, April 4, May 5, June 6, July 7, August 8, September 9, October 10, November 11, or December 12. You may not notice you've interchanged the month and day in your algorithm."

(You probably don't need to worry about January 1, since it's a holiday ...)

And one day early this month, *I* learned that it's also a good idea to test a program both during and after the first 9 days of the month. Gotta watch those 1- and 2-digit numbers!

(And during both of the periods January-September and October-December...)

Mark Brader, Toronto utzoo!sq!msb msb@sq.com
"If the standard says that [things] depend on the phase of the moon, the
programmer should be prepared to look out the window as necessary." Chris Torek

not so easy to be anonymous

Robert L Ullmann <ariel@world.std.com> Tue, 9 Nov 1993 22:39:12 -0500

In <u>RISKS-15.19</u>, Steven S. Davis points out that anonymous remailers (at least the one at anon.penet.fi) remove signatures beginning with -- lines. But

there is a much more effective signature.

On the two occasions that I have been curious enough to investigate the real identity of anonymous posters I have had no difficulty identifying them with a bit of searching about. Both of the people I was looking for had posted signed messages in the same or nearby groups, and were readily identified. How? Consider Steven's text:

"In Risks 15.17, an32153@anon.penet.fi remarked upon the dangers of including a signature with anonymous postings. It's not quite as absurd as it seems, if someone uses a mailer that appends the signature automatically (I can't imagine that anyone who cared about their anonymity, as opposed to those who just are assigned an anonymous id because they reply to somebody who uses one, would deliberately append a revealing signature). The solution to that, at least on anon.penet.fi, is simple: The server considers anything after a line beginning with two dashes as a signature and cuts it off (this can be a complication if someone tries to append a document to a message and uses a row of dashes to separate it from the main text). So if you want to send mail anonymously, either dump your signature or be certain it starts with --."

Now, look at the style:

- 1) he has a unique habit of adding spaces after (and before).
- 2) the paren clauses come at the end of sentences. They are not dependent clauses, and the . comes outside the)
- 3) he uses commas before dependent clauses. (cf last sentence)

The meter is distinctive. (Read it aloud without paying attention to the words.) Ta-d-d-d-d, COMMA, d-d-d-d-d-d (Ta-d-d-d-d-d, COMMA, ta-d-d-d-d-d-d). Ta-d-d-d-d-d, COMMA, d-d-d-d-d-d (Ta-d-d-d-d-d-d, COMMA, ta-d-d-d-d-d-d-d-d-d-d-d).

I'm not picking on Steven; anyone who doesn't write in a formal, carefully corrected prose style will get caught by this.

It is real easy. And not so easy to really be anonymous.

[PGN adds: By the way, you might have mentioned line lengths. (But I use a standard of 78 for RISKS, so that the people who add "<" do not overflow, and I usually reblock longer or shorter lines.) I also usually neutralize the time zone on authored mailings to RISKS for which the author wishes to remain anonymous. You also did not mention giveaway mispelings. (I try to run every issue through a speling corekter.) As Tom Lehrer once wrote RISKS-11.48>,

Don't write naughty words on walls that you can't spell.]

★ The Snakes of Medusa and Cyberspace: Internet identity subversion

"L. Detweiler" <ld231782@longs.lance.colostate.edu>

Tue, 02 Nov 93 23:52:05 -0700

I have long tracked the Internet debates on identity issues, such as anonymity, with zeal and commitment. Recently I have become very alarmed by the very serious potential RISKS of a practice I've termed 'pseudospoofing'.

In short, there are a few basic categories under which identities may fall under in Cyberspace. (This is not a comprehensive list.)

'True Name' -- a person sends a message under their legal identity.

'Anonymously' -- features of the message indicate it could be from anyone. One such feature would include origination from an anonymity server, such as the now-famous Finnish server anon.penet.fi, operated for nearly a year by J. Helsingius.

'Pseudonymously' -- features of the message indicate it was issued under a pseudonym other than a True Name. One might build up a reputation under different pseudonyms. In a technical sense, anon.penet.fi aliases are pseudonyms.

The above categories are well recognized, established, and even all largely entrenched on the Internet. However, another distinct category exists:

'Pseudoanonymously' -- the message identification is of a 'fake' identity, a person that does not exist despite the implicit indications of the message (such as a signature with a realistic name, including a phone number, etc.)

Note that pseudoanonymous postings are unequivocally a form of *active* deception that transcends the *passive* concealment of anonymity, and therein lies the danger. If I posted under the name Jim Riverman and set up a unique phone number for the basic purpose of fooling others into thinking that Jim Riverman was a unique person from myself, many very dark machinations of human trust are possible.

A message that is anonymous could be 'from anyone', including a known megalomaniac, and people would be cautious in revealing information to that nonentity -- and are encouraged to speculate on it. (I have advocated and championed this form of anonymity on the Internet.) But someone who supposedly 'exists' automatically carries more implicit trust -- including a very important kind of trust that they are unique from other individuals. I think some social parasites increasingly are exploiting the tradition of openness and honesty on the Internet to prey on others via this technique of pseudospoofing, and that newer, more vicious and insidious forms are evolving.

* * *

For example, I could post public messages under the Jim Riverman identity saying that L. Detweiler is the most eminent authority on anonymity issues the Internet has ever seen. I could rip apart other's public arguments that criticize L. Detweiler and get everyone else to argue about irrelevant details -- an ingenious way to 'change the subject' by derailing it with dynamite. This would all be highly effective if I built up an independent reputation as Jim Riverman with periodic, highly refined posts on software engineering or

some other topic of interest. And others might become unwitting accomplices to the deception by quoting sentences or articles by Jim Riverman in their own articles appearing in the same place or other more reputable forums, such as RISKS.

These are just some of the alarming uses of pseudospoofing in *public* environments, which I think most reasonable people would agree, depending on the context and medium, are highly damaging to community trust, and furthermore dishonest, immoral, and unethical. At the bare minimum, others should be informed if it is occurring, or they may feel victimized by a bizarre social experiment on unwilling and unsuspecting participants.

However, there are far more disturbing evils possible with use of pseudospoofing in *private* email. I could contact others in email under the identity Jim Riverman and ask them, `What do you think of L. Detweiler, anyway?' I could even become an apologist for L. Detweiler under Jim Riverman. `Dorothy, I really respect your contributions, but you are way out of line on this one. L. Detweiler is a really nice guy. I've met him personally.' (One Cypherpunk member called some of these uses the `intersection' of pseudonymous identities.)

Even further, I could use this technique as a powerful espionage method of a turncoat, agent provocateur, or double agent in eliciting valuable information from anyone trusting and unsuspecting. One method to build up trust (and perhaps the most basic way) is to provide relevant, valuable information, and then ask for some `in return for the favor.' E.g. Jim Riverman says to the Cyberspace Police, `Yes, I heard L. Detweiler is getting some major heat over his pseudospoofing postings. In fact, he started subscribing to the Criminal Techniques mailing list. What are you guys going to do with him, anyway?' Again, if the message is pseudoanonymous as opposed to anonymous, even with a built-up online reputation, the trap is dangerously plausible.

Note that 'digital signatures' alone do not solve this problem of ensuring that identities correspond to real people. A 'true' signature, e.g. a written one, has the property that it is unique to a given individual, outside of illicit forgery. But it is quite feasible for a pseudospoofer to maintain multiple digital signatures and juggle them readily among a large arsenal of fake identities. In this sense what many are calling 'digital signatures' are really just 'identification tags' if they lack corresponding mechanisms to ensure correlations to actual human identity, e.g. relation to birth certificates or any of the other mechanisms our society has evolved over centuries to authenticate real identities.

* * *

Many jaded readers are probably thinking at this point that they have already seen some of these subversive uses of pseudospoofing and are not alarmed by my scenarios so far. But the uses of pseudospoofing that most alarm me, and form the basis for my article here, are the extremely dangerous, insideous, and treacherous refinements of this technique that could lead to far more serious 'real world' consequences outside of the loquacious frivolity of, say, most of Usenet. These are related to the potential of waging a systematic campaign of propaganda, disinformation, or brainwashing unleashed on an unsuspecting public by a subversive organization.

Suppose that a criminal group called the CryptoAnarchists wished to take over the Internet and future Cyberspace, and promote their agenda of pseudospoofing as a way of aiding criminal behaviors such as tax evasion, black marketeering, and general destabilization of governments, democracy, laws, and law enforcement, partly with the aid of pseudospoofing techniques. Unfortunately, the technique of pseudospoofing itself, coupled with the Internet's extreme vulnerability to it, could be used as an extremely powerful tool in accomplishing their goal of cyberspatial domination.

The CryptoAnarchists would first seek to consolidate their supporters in a secret society with very strict membership requirements. They could have a secret mailing list that reaches all of those in the group, from which to plot in secret their activities `in the open'. The secret mailing list would be dedicated to insiders describing their activities, such as the new fake identities they have succeeded in acquiring, who is in charge of which identities, coordinating the software and databases used to prevent `crossings', or leaks that reveal a link between pseudospoofed identities, and gauging the extent of seized domains and `new territories' to be invaded.

The CryptoAnarchists require public manipulation to achieve their ends, however. For this purpose they would find a public mailing list extremely useful. They would promote themselves on this mailing list through the techniques of pseudospoofing, perhaps even to the extent of misleading reporters and obtaining favorable media accounts in newspapers or magazines. They would find it useful to disguise their agenda, of course, say under the guise of `privacy for the masses' or `the cryptographic revolution.' They might post fake status reports of ongoing `real-world' projects and have insiders confirm them to increase the prestige and respectability of the organization. `Eric May' says, `Oh yes! We are very far along on the anonymous digital cash server!' `T.C. Hughes' says, `Oh yes! I saw the server yesterday! A fine piece of machinery!' They might consistently talk about the beautiful consequences of `pure and true anonymity' when really referring to pseudoanonymity and pseudospoofing.

In fact, they might develop an entire mythology, philosophy, even *religion* that promotes pseudospoofing as a liberating capability, and refine and espouse it on their public mailing list. This might include, for example, elevating instances of multiple personality disorder to legendary virtuous status. They would consistently talk about famous science fiction by respected authors that refers to the blurring of identities, even though it would not really specifically address the issue of pseudospoofing, and implying that it did was just another obfuscatory fabrication. The disinformation campaign would be self-reinforcing: even outsiders, 'real people', could themselves become independent proselytizers after being sufficiently converted.

In promoting this philosophy, they would use the techniques of brainwashing and an illusion of peer pressure to manipulate unknowing subscribers. If any subscriber expressed any doubt, the CryptoAnarchists could wage a concerted campaign of mental assault on the victim both on the public mailing list and in private email, to the point that real people would feel isolated, alone, and unsupported -- but only because of the perceived consensus of nonexistent identities.

Even more treacherously, they could target individuals who suspect the existence of conspiracies by disparaging, discouraging, and discrediting them publicly and privately as 'paranoid ranters' and 'conspiracy theorists'. They would say that while pseudospoofing is possible, it is certainly not widespread, no non-Draconian mechanisms could be implemented to prevent it, and besides, people shouldn't be 'punished' for the misdeeds of a few, no one really takes the Internet seriously anyway, people aren't really influenced by propaganda and 'peer pressure', and pseudospoofing is simply a 'fact of life' of cyberspace. The arguments would usually be couched in the terms of moral relativism. 'Hal Dinkelacker' says, 'is anything *really* inherently evil? everyone *I've* met who thought so was a fascist!'

The CryptoAnarchists might even be able to make a real-world pariah from simulated ire and criticism directed at a single strong opponent, say, L. Detweiler, from many simulated identities in cyberspace, who are mistaken to be other real, reputable people by L. Detweiler's cyberspatial and real-world associates `under the influence' of the mailing list or other infected outlet, who consequently shun him in both realms.

Unfortunately, because the CryptoAnarchist techniques are so readily concealed, evidence for their conspirational [sic] machinations would be extremely difficult to detect and obtain. When one `tentacle', or fake identity, is discovered, they would simply `cut it off' (stop using it, and dissociate themselves) with no fatal loss to the continued growth of the overall body. Before that, however, they might engage in further disinformation attacks to prevent the `exposure'. I might send information as L. Detweiler to Dorothy saying, `Dorothy-- what makes you think Jim Riverman does not exist? I've met him personally. There are others who can attest that he is real. You are doing nothing but inventing elaborate, insane fantasies by believing otherwise.'

Also in this manner of conspirational manipulation, they would find it very useful to subscribe to, or rather infiltrate, very many Internet mailing lists, particularly those that are extremely sensitive and dedicated to developing Internet protocols, and related to identification and email, such as SMTP (Simple Mail Transfer Protocol), PEM (Privacy Enhanced Mail) or DNS (Domain Name Service). They could find others with queries from another tentacle, say 'Nick Chandler', in the form, 'does anyone know of lists dedicated to identification protocols? please email me.'

Once subscribed, the CryptoAnarchists could use the aforementioned techniques of pseudospoofing to build up the reputations of their tentacles and manipulate others with those tentacles. If someone suggested a robust protocol for identification on one of these mailing lists, they could engage a single or even multiple tentacles into sabotaging the proposal with scathing criticism and derailing discussion into irrelevant areas. They could bombard the particularly strong supporters of identity mechanisms with a barrage of flames in the victim's private mail box, with many similar messages from seemingly unique identities saying, in slight variations. 'Greg Landry' says, 'I respect what you've done so far in so-and-so area, but your ideas on preventing pseudospoofing are just way too impractical, Draconian, undesirable, and unpleasant, and I think you should give up pursuing them. You've really gone off the deep end. The cat is out of the bag on the Internet

and there's just no way to go backwards.'

In fact, the CryptoAnarchists might even infiltrate sensitive internal mailing lists like those maintained by CERT (Computer Emergency Response Team). This would be roughly analogous to a criminal gaining access to insides of the telephone system or a police station. They would be informed ahead of time of law enforcement's knowledge of their conspiracies, and may even be able to thwart their investigations and countermeasures with further insidious manipulations. They might even subvert the existing Internet SMTP and DNS identification databases. In a sense, the overall effect would ultimately be as devastating as AIDS, like a virus invading the protective and defensive machinery itself designed to stop contagious infections. Once a few snakes of Medusa had their fangs into Cyberspace, an antidote to the invisible, spreading, self-reinforcing poison would be virtually impossible to administer -- Medusa would certainly do *anything* to avoid swallowing it!

* * *

I have become aware of these serious abuses possible with pseudoanonymous posting from my long affiliation with the Cypherpunks, an allegiance I have now severed because of my realization of their basic hidden agenda in promoting the practice of pseudospoofing, or using pseudoanonymous identities in the aforementioned ways to manipulate and systematically deceive others in cyberspace. I urge others involved with the group to reconsider their own affiliation and crystallize their own position on pseudospoofing.

In 'exposing' this practice of pseudospoofing I have written much material, including an essay entitled 'The Joy of Pseudospoofing' which I will make available to anyone who contacts me in email. Also, results of an informal survey will be available in a few weeks. For the highly literate and technically savvy RISKS readers I would like to simply point out some of the most treacherous and insidious uses of this practice -- which, in my view, constitutes an extant, active, slow-creeping poison spreading over the Internet. Unfortunately, as evidence in this claim I cannot be more specific than the previous seemingly fictional account, except to offer an assurance that it is based on true events in my own mailbox in particular, and perhaps on the global Internet in general (I fervently hope energetic and ingenious readers with more resources than I can fill in the blanks, and perhaps become effective pseudospoofed ghost exorcists.)

While many will brand me a frothing alarmist, on the other hand there are absolutlely no mechanisms anyone can point to on the Internet that discredit my scenario -- quite to the contrary, its decentralized, unregulated, and open-access traditions validate it -- and the rhetorical question `who could possibly be depraved enough to do all this?' is intended to be answered by this article! Particularly when the Internet is being used for increasingly deathly serious endeavors such as Presidential opinion gathering and commercial activities, I pray that disastrous reliance is never entrusted to the security of phantoms.

In writing this I hope to

- alert others, particularly those with noncasual scientific and professional

interests in the Internet, to the existence and evils of pseudospoofing, its potentially deadly flourishing status, and to be alert for personal encounters with it

- help delineate the `rights' and `recourses' of Cyberspatial participants related to pseudospoofing, particularly with the view of the Internet as a model for future cyberspace -- for example, does everyone at least have the `right' to bar pseudospoofed identities from their own mailbox? to form mailing lists that outlaw it?
- help establish at least a strong, universal taboo against pseudospoofing among those in the online community, particularly the occurrence of 'intersections', hopefully on the strong level of the current widespread repulsions for censorship
- encourage others to develop procedures, algorithms, and protocols to dampen the treacherous and toxic effects of pseudospoofing where appropriate, particularly sensitive mailing lists relating to serious project or Internet development efforts
- energize a strong resistance against those who criticize these noble aims of making cyberspace more honest and hospitable via identity and authentication mechanisms
- alert others to the possibility of apologists and reactionaries for the 'fluidity of identity on the Internet' who may themselves be pseudospoofed phantom tentacles
- alert others to the possibilities, dangers, and perversions of 'infiltrations' into mailing lists, particularly of a systematic and widespread campaign
- urge those running mailing lists to condemn pseudospoofing and require promises to refrain from it as part of membership requirements, and urge members to police each other
- urge anyone conducting surveys or polls on the Internet to view results with extreme prejudice or use greater authentication techniques than mere reliance on email addresses and signatures alone, because of the possibility of increasing, concerted, poisonous pseudospoofing
- hear from others more systematic and scientific measurements and analyses on the degree, and ramifications of, and preventive measures for pseudospoofing on the Internet, particularly on the possibilities and vulnerabilities of SMTP and DNS database subversions (maybe a mailing list dedicated to the subject of thwarting pseudospoofing could be started)
- promote the general area of identification and authentication as a scholarly research subject of the utmost importance, in resolving a key, even primary and paramount element of the current 'ideal future cyberspatial infrastructure' debate
- "That which can never be enforced should not be prohibited. The claim that a person should have only one pseudonym per forum indicates profound

misunderstanding. If someone wants to have multiple ... pseudonyms, they will be able to; that is one of the main goals of cypherpunks software. The situations you despise will occur. This is reality. Change your own psychology or change your own software. You will not be able to change the other person." --E.Hughes, cofounder, Cypherpunks

"Better to live with the occasional vagaries of digital pseudonyms than to ban them." --T.C.May, cofounder, Cypherpunks

"In a false quarrel there is no true valour." --Shakespeare

"Propaganda is to democracy what violence is to totalitarianism." --N. Chomsky

"Oh what a tangled web we weave, when first we practice to deceive." --Sir Walter Scott

"I'm not going anywhere. I like it here." -- Snake #7

I thank the following eminent Cypherpunks for ideas in this article, although it should not be construed to be representative of their opinions, and neither can I provide any guarantee they represent unique people:

G.Broiles, A.Chandler, J.Dinkelacker, H.Finney, E.Hughes, M.Landry, T.C.May, N.Szabo

Notes:

- 1) human-readable subscription requests to E.Hughes' Cypherpunks mailing list go to cypherpunks-request@toad.com.
- 2) a treatise on the history and psychology of anonymity on the Internet (but not specifically pseudoanonymity) can be obtained from rtfm.mit.edu: /pub/usenet/news.answers/net-anonymity. Some other areas related to this article are covered in [...]/net-privacy.
- 3) The Cypherpunk archives, including their charter and many documents overtly relating to anonymity (covertly to pseudoanonymity), can be obtained from soda.berkeley.edu:/pub/cypherpunks.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 26

Saturday 13 November 1993

Contents

Gripen crash report

Urban Fredriksson

SAS MD-81 crash report, December 1991

Martyn Thomas

MASS state police confuse car owners with gun carriers (NOT)

Simson Garfinkel

Re: No change in Ada policy

Anonymous

Parnas

Risk-happy drivers foil anti-lock brakes

Mark Brader

Naissance d'un virus soon to be published

Jean-Bernard Condat

Re: pseudospoofing

Andrew Marchant-Shapiro

I'm Me

Nick Szabo

Re: anonymizing service

Karl Lui Barrus

Re: Not so easy to be anonymous

Seth Chazanoff

Re: Stupid language games

Dave Parnas

Re: Networking

Phil Agre

"Friendly Fire" in system design

Steve Taylor

Re: Teachers Beware!

Andy Cunningham

FBI Operation "Root Canal" Documents Revealed

Dave Banisar

Info on RISKS (comp.risks)

Gripen crash report

Urban Fredriksson <urf@icl.se> Sat, 13 Nov 1993 07:23:58 GMT

The Swedish Accident Investigation Board's preliminary report on the Gripen crash on Aug 8 is presented in the air force's magazine FlygvapenNytt 3/93. Summarily, the conclusions are:

- The only equipment malfunction before the crash was the electronic map which had nothing to do with the crash
- The flight control system, the engine and all other systems worked as specified until the aircraft impacted
- No external cause is suspected
- The pilot was properly trained and equipped
- The limits for minimum altitude and maximum angle of attack were exceeded insignificantly and did not have anything to do with the crash
- The manufacturer and customer knew that large and rapid stick movements could cause divergent Pilot Induced Oscillations, but considered the likelyhood of it actually happening insignificant, so all pilots weren't informed
- The red warning light was too late in telling the pilot that the control system was saturated, for him to do anything about it
- The low altitude of 270 m made it impossible for the pilot to try to regain control

The crash sequence started with a low speed 360 deg left turn at 280 m. The afterburner was lit, speed 285 km/h, load 2 G, bank angle 65 deg and angle of attack 21 deg. After finishing the turn, the control stick was moved to the right almost to the endpoint and slightly forward. The left wing's rear control surface rapidly went to the bottom position. The aircraft to bank to the right 20 deg past horizontal, angle of attack decreased to less than 10 deg. In order to fast regain a horizontal wing attitude, the pilot rapidly pulled the stick almost all the way to the left and continued to keep it slightly forward.

This caused the control surfaces to move with their maximum deflection speed, and as the flight control system then had little or no control surface movement on its own to work with, the stability margin was reduced. At the same time the alert system informed the pilot of this, and he no longer recognized the aircraft's behaviour.

The aircraft started to roll to the left and pitch up. In response to this the control stick was moved almost to the right endpoint and some forward. The result was a roll to the right to 35 deg bank and a lowering of the nose to 7 deg below the horizon, whereupon the stick was pulled forcefully back and to the left. At the same time, the artificial stability system tried to raise the nose, which in combination with the pilot's command caused a powerful pitch up. By this time, the control stick was fully forward, but the aircraft was already unflyable.

>From exit of the turn until ejection the sequence took 6.2 s. The time from when the pilot didn't recognize the flying characteristics until stall took 2.7 s, but the control system warning wasn't shown until 1.2 s before the stall.

The cause of the crash was the misjudgements that PIO was so unlikely and that the warning light would tell about any problems early enough for no mention of this in the pilot's manual was necessary.

My own comments: The first crash was caused by the artificial control system having too much authority, sometimes leading to a slight response delay to the pilot's commands, causing PIO during a landing in gusting sidewinds. It has been reported from other sources that the main change made to the control laws a few weeks before the crash was to increase the pilot's authority a tiny bit.

Some doubt has also been cast on the statement that the flight control computer worked as specified, as its log only goes a few seconds back and thus only showed data since the pilot left the aircraft. The crash report doesn't go into this in detail, but it is clear they had its error log to work with, in addition to data from the "black box".

This report also clears up some things I didn't understand from earlier this year, when it was said that maximum angle of attack was 26 deg, and at 35 deg the rear airbrakes come out and the canard gives a full pitch down command automatically. Obviously fly-by-wire does not have to mean you impose hard limits on the aircraft's performance, in the Gripen case the pilot is trusted not to exceed them.

Urban Fredriksson urf@icl.se

SAS MD-81 crash report, December 1991

Martyn Thomas <mct@praxis.co.uk> Fri, 12 Nov 1993 10:11:58 +0000 (GMT)

According to Flight International, 10 NOVEMBER 1993, "an automatic engine-control function in the McDonnell Douglas MD-81, of which the operating airline was unaware, was a major factor in the Scandinavian Airlines System (SAS) accident near Stockholm, Sweden, in December 1991, says the official report into the accident"

In summary, it seems that the airline failed to detect clear ice on the wings before takeoff. The ice broke free and entered the engines damaging the fan stages. This caused the right engine to surge. The pilots retarded the right throttle. The automatic thrust-restoration system ATR caused both throttles to advance without the pilots noticing, making the surging worse in the right engine and starting surging in the left. The surges destroyed the engines.

It seems that SAS were unaware of the ATR, which was documented but in a section of the production flight-procedure manual dealing with noise abatement. SAS VP Johan Juhlin is reported as saying "We did not order it. It was hidden in the computer. The only way to disconnect the ATR was to disconnect the whole autothrottle system."

McDonnell Douglas say that they made SAS aware of the full capabilities of

the MD-80 when it was delivered.

The documentation has since been improved, and SAS have changed their procedures and training to emphasise the ATR and correct anti-surging procedures.

The ATR was designed to improve safety where an engine fails after take off and noise abatement procedures have caused the engines to be throttled back.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

✓ Massachusetts state police confuse car owners with gun carriers (NOT)

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Wed, 10 Nov 93 20:19:58 -0500

I forwarded the RISKS note about people receiving gun permit renewal notes accidentally in Massachusetts to David Lewis, who heads the Registry of Motor Vehicle's information technology group. (His official title is Deputy Registrar.)

You may remember the message:

>Date: Fri, 5 Nov 93 13:26:43 EST

>Subject: Mass. state police confuse car owners with gun carriers

>My wife received a letter yesterday from the Massachusetts state police, >informing her that it was time to renew her "License to Carry Firearms". >It included a renewal form that she was to take to her local licensing >authority, the police station in our case.

This is what David Lewis had to say about it:

"It wasn't actually a tape of vehicle owners. They got stickers confused with people who were supposed to get food stamps. So the people [who were supposed to get] the food stamp books got the gun permits, and the people who were supposed to get gun permits got food stamps. But it wasn't the Registry this time."

Just setting the record straight.

★ Re: No change in Ada policy (Eachus, RISKS-15.25)

"ANONYMOUSLY INCLUDED via Peter G. Neumann" <neumann@csl.sri.com> Fri, 12 Nov 93 8:57:55 PST

[This was submitted by a reliable RISKS contributor who wishes to remain anonymous. PGN]

It was noted in <u>RISKS-15.25</u> that industry needs to be sold on the usage of Ada

As far as I know, industry likes Ada well enough. What they do not like is the EXCLUSIVE use of Ada. Industry has the problem of maintaining millions of lines of working code, code that is rather well debugged, and reasonably well documented, code that was written in what was once a DoD standard - FORTRAN or COBOL, for example.

If the government really believes in capitalism, and if the government believes that private industry is in business to make money, then the government should be willing to allow industry to transition to Ada as that makes economic good sense. And not sooner.

What such a policy shift might discover is that there are real problems for which Ada is not the best language.

There is a very significant difference between a policy of "Ada exclusively" and a policy of "any assembly language you choose." Limiting government sponsored software to a list of government approved languages is a good place to start; investing some r&D money (little "r" and big "D" since most of the "research" is done) in software engineering "tools" for some "legacy languages" (FORTRAN, COBOL, BASIC) would improve the codes written in those older languages, and avoid the impact of a massive mandated change. Indeed, some of these "tools" exist; "DAVE" for FORTRAN, for instance.

★ Re: No change in Ada policy (Eachus, RISKS-15.25)

Dave Parnas <parnas@triose.eng.mcmaster.ca> Thu, 11 Nov 93 22:05:19 EST

Was there anything significant in your running the expression of faith in ADA just before the article about Groundhog day? There are still people who seem to believe in the latter too.

Dave

★ Re: Risk-happy drivers foil anti-lock brakes (Bruce, RISKS-15.24)

Mark Brader <msb@sq.sq.com> Wed, 10 Nov 1993 19:40:28 -0500

- > From the Ottawa Citizen Sunday Edition November 7, 1993
- > by Brad Evenson, Citizen consumer writer

> ..

- > "After having practised the emergency stopping manoeuvres with anti-> lock brakes, drivers drove faster, had higher accelerations around a curve > and stopped harder," a summary of the study said.
- > "If drivers choose to drive faster because they know they have greater > control, and if they choose to follow other vehicles more closely under > slippery road conditions, then the safety benefit from anti-lock brakes

> might be reduced or lost completely."

Okay, if this study is not misleading, then anti-lock brakes are a device which allows faster driving and closer following in slippery road conditions, without increasing the accident rate. This is bad?

Mark Brader, SoftQuad Inc., Toronto utzoo!sq!msb, msb@sq.com

Naissance d'un virus soon to be published :-)

cccf <cccf@altern.com> Wed, 10 Nov 93 11:08:44 EST

By the general secretary of the Chaos Computer Club France (CCCF), the French translation of "The Little Black Book of Computer Viruses" will soon be published by Addison-Wesley France (fax: +33 1 48 87 97 99).

Naassance d'un Virus (dec 1993, 237 pages, circa 98 FF).

Jean-Bernard Condat, PO Box 155, 93404 St-Ouen Cedex, France Phone: +33 1 47874083, fax: +33 1 47874919, email: cccf@altern.com

★ RE: pseudospoofing (RISKS-15.25)

"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu> 10 Nov 93 20:07:00 EST

On pseudospoofing, there is an interesting SF-based discussion of the potential political consequences, to be found in Orson Scott Card's _Speaker_for_the_Dead_ (if I recall correctly, the two other sections of the [so far] trilogy also contain some elements: _Ender's_Game and _Xenocide_). In these books, Card describes a situation in which the political commons (not unlike internet) is invaded by two extremely bright pseudospoofers, who, seemingly opposed, debate each other in such a way as to manipulate the public into going along with their schemes. There are better writers than Card, and the concept has probably been around for a while, but it's an interesting execution.

Andrew Marchant-Shapiro Depts of Sociology and Political Science USmail: Union College, Schenectady NY 12308 AT&T: (518) 388-6225 INTERNET: marchana@gar.union.edu BITNET: marchana@union.bitnet (no fooling!)

[AM-S among others reminded me that my rend(er)ing of Tom Lehrer was not as on the records. "Don't write naughty words on walls IF you can't spell."

I knew that, but (mis?)remembered a live version from the early 50s... PGN]

I'm Me

Nick Szabo <szabo@netcom.com> Thu, 11 Nov 93 0:28:31 PST

I'd like to assure the readers of RISKS that I am in fact a unique person, distinct from the other names L. Detweiler listed. Of the people on his list I know from personal contact, all are distinct people in Real Life(tm). Well before his post to RISKS, L. Detweiler was provided means of personally verifying that many of the names he listed are distinct True Names (eg phone numbers he can call), but it doesn't seem to help.

Nick Szabo szabo@netcom.com

★ Re: anonymizing service

Karl Lui Barrus <klbarrus@owlnet.rice.edu> Fri, 12 Nov 93 09:42:55 CST

To everybody who is worried about the service anon.penet.fi:

If you mail to an address such as an####@anon.penet.fi, you will be assigned an id.

If you mail to na####@anon.penet.fi, your message will be passed along and you will NOT be assigned an id.

an == anonymous
na == not anonymous

It's that simple. I mention this because it seems every other week somebody is discovering the "risks" of this service while how to avoid the problem altogether is never discussed.

★ Re: Not so easy to be anonymous (Ullman, RISKS-15.25)

Seth Chazanoff <seth@inst-sun1.jpl.nasa.gov>
11 Nov 1993 17:17:01 GMT

In RISKS-15.25, Robert L Ullmann points out that one may be able to be identified when using an anonymous mailer through stylistic analysis techniques. (This is what radio intercept operators in WWII called the senders fist.), There is a section that I was told about on the Comparative Literature GRE that starts _None of the following paragraphs were written by any of the authors listed, but the correct answer is the name of the author whose style the paragraph was written in._ The problem with this technique is that many people may use similar enough techniques that attempting to assign a message to an individual may be very difficult.

Recently JPL opened an anonymous newsgroup for internal gripes. My boss's boss came to me and said that he had noticed that I was active in that group. (It is good to know that management is reading the group. :-)) I asked him how he came to that conclusion and he told me that he recognized my style of

writing. The only problem was I had not heard of that newsgroup till he told me about it.

Seth

★ Re: Stupid language games (Schroeppel, RISKS-15.24)

Dave Parnas <parnas@triose.eng.mcmaster.ca> Thu, 11 Nov 93 22:00:44 EST

Neither Jones, nor Mellor, nor Parnas (see RISKS-15.22) was arguing in favour of exhaustive testing in the quote picked upon by Schroeppel. Jones was trying to explain the complexity of software to non-programmers. He did this by trying to give the listeners a "feel" for the number of possible cases that would have to be considered. I pointed out that even though the complexity, as described, seemed daunting, it was understated. There is neither theoretical, nor practical basis for focusing on control state and neglecting data state. The thought attributed to Daimler by Schroeppel is irrelevant because carburetors don't have to be tested on all mixtures, just the ones that they will encounter, and that can be controlled. Moreover, continuity, and known upperbounds on the derivatives of the functions describing carburetors, limit the amount of testing that need be done. It's this lack of continuity that makes testing of software so difficult.

✓ Re: Networking

Phil Agre <pagre@weber.ucsd.edu> Wed, 10 Nov 1993 16:48:21 -0800

Richard Schroeppel <rcs@cs.arizona.edu> has taken exception to my essay on "Networking on the Network" in Risks 15.12, stating "I do not choose my friends based on their potential usefulness to my professional advancement. Even a little bit." As my essay repeatedly made clear, I am not advising anybody on the choice of their friends, only on the development of their professional relationships. These are different concepts.

Heretofore, practical knowledge about how the world works has been restricted to elites, who are so embarrassed about this knowledge that they only pass it along in private, leaving others exposed to the Risks of untutored navigation in the professional world, permanently wondering why they can't seem to get anything done. If we write down the world's unwritten rules and circulate them on the Internet, maybe we can level the playing field a bit -- or even change the rules.

Phil Agre, UCSD

"Friendly Fire" in system design

Steve Taylor <smt@xedoc.com.au>

Fri, 12 Nov 93 18:14:15 +1100

I've just remembered an old episode of the "Space Patrol" TV series in which the good guys spaceship was fired on by Earth spaceport defenses, which had been set to fire on any metals not originating on Earth.

Unfortunately in a classic design glitch, the system designers had forgotten that many of the Space Patrol's ships had been built on Pluto, and were made of - ahem... Plutonium.

The RISKS are obvious. Whatever they are.

Steve Taylor smt@xedoc.com.au Xedoc Software Development

★ Re: Teachers Beware! [Spera, RISKS-15.23]

"Your friendly UNIX guru" <andyc@cappsdv2.fob.ford.com> Fri, 12 Nov 93 08:53:24 +0000

- > First there was writing in the palm of the hand, then the crib sheet (or back
- > of the tie or sole of the shoe or etc.), next came the programmable
- > calculator, now coming to a store near you, the Newton generation.

There was an alleged incident at Reading University (England) where a student used a laptop computer in an exam. The exam in question was "open book" but the rules did not forbid it's use in any exam. After this, the rules were tightened up and each calculator had to be "certified", as either - "non programmable" or "programmable and memory cleared". Certificates had to be displayed on desks, and invigilators could request that the memory be cleared at the start of the exam. Any device with alphanumeric memory was prohibited. Any calculator (even a simple 4 function credit card calculator) could be confiscated until the end of the exam unless a certificate was displayed on the desk.

I can't vouch for the accuracy of the incident, but I was very aware of the rules being tightened up to the point that I had to go and buy a simple scientific calculator to use instead of my HP-28S. And switching from RPN to grungy-old-horrible-notation was a total pain!

Highlighting the flaws in a set of rules isn't always a good idea - it usually gets the rules tightened too far.

AndyC the WB (aka Andy Cunningham) Logica Industry / Ford Motor Company Phone: +44 277 253765 Fax: +44 277 253582 Net:andyc@cappsdv2.fob.ford.com

✗ FBI Operation "Root Canal" Documents Revealed

Dave Banisar <banisar@washofc.cpsr.org> Sat, 13 Nov 1993 08:40:25 -0500

(from the CPSR Alert 2.05)

In response to a CPSR Freedom of Information Act lawsuit, the FBI this week released 185 pages of documents concerning the Bureau's Digital Telephony Initiative, code-named Operation "Root Canal." The newly disclosed material raises serious doubts as to the accuracy of the FBI's claim that advances in telecommunications technology have hampered law enforcement efforts to execute court-authorized wiretaps.

The FBI documents reveal that the Bureau initiated a well-orchestrated public relations campaign in support of "proposed legislation to compel telecommunications industry cooperation in assuring our digital telephony intercept requirements are met." A May 26, 1992, memorandum from the Director of the FBI to the Attorney General lays out a "strategy ... for gaining support for the bill once it reaches Congress," including the following:

"Each FBI Special Agent in Charge's contacting key law enforcement and prosecutorial officials in his/her territory to stress the urgency of Congress's being sensitized to this critical issue;

Field Office media representatives educating their contacts by explaining and documenting, in both local and national dimensions, the crisis facing law enforcement and the need for legislation; and

Gaining the support of the professional associations representing law enforcement and prosecutors."

However, despite efforts to obtain documentation from the field in support of Bureau claims of a "crisis facing law enforcement," the response from FBI Field Offices was that they experienced *no* difficulty in conducting electronic surveillance. For example, a December 3, 1992, memorandum from Newark reported the following:

The Newark office of the Drug Enforcement Administration "advised that as of this date, the DEA has not had any technical problems with advanced telephone technology."

The New Jersey Attorney General's Office "has not experienced any problems with the telephone company since the last contact."

An agent from the Newark office of the Internal Revenue Service "advised that since the last time he was contacted, his unit has not had any problems with advanced telephony matters."

An official of the New Jersey State Police "advised that as of this date he has had no problems with the present technology hindering his investigations."

Likewise, a memorandum from the Philadelphia Field Office reported that the local offices of the IRS, Customs Service and the Secret Service were contacted and "experienced no difficulties with new technologies." Indeed, the newly-released documents contain no reports of *any* technical problems in the field.

The documents also reveal the FBI's critical role in the development of the Digital Signature Standard (DSS), a cryptographic means of authenticating electronic communications that the National Institute of Standards and Technology was expected to develop. The DSS was proposed in August 1991 by the National Institute of Standards and Technology. NIST later acknowledged that the National Security Agency developed the standard. The newly disclosed documents appear to confirm speculation that the FBI and the NSA worked to undermine the legal authority of the NIST to develop standards for the nation's communications infrastructure.

CPSR intends to pursue further FOIA litigation to establish the extent of the FBI involvement in the development of the DSS and also to obtain a "cost-benefit" study discussed in one of the FBI Director's memos and other documents the Bureau continues to withhold.

To subscribe to the Alert, send the message:

"subscribe cpsr



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 27

Tuesday 17 November 1993

Contents

Re: The Snakes of Medusa and Cyberspace

mathew

Alex Glockner

Perry E. Metzger

Jamie Dinkelacker

Arthur Abraham

Peter Leppik

Brad Hicks

Neil McKellar

Leonard Mignerey

L. Detweiler

Info on RISKS (comp.risks)

★ Re: The Snakes of Medusa and Cyberspace (RISKS-15.25)

mathew <mathew@mantis.co.uk> 11 Nov 1993 12:13:34 -0000

"L. Detweiler" <ld231782@longs.lance.colostate.edu> writes at length about the evils of what he calls "pseudoanonymous posting". I shall try to keep this reply brief. I am interested not only in the issue of pseudonymity, but in the structure of Detweiler's allegations. His posting appears to me to be an artfully crafted conspiracy theory.

He begins by defining "pseudoanonymously":

>`Pseudoanonymously' -- the message identification is of a `fake' identity, a >person that does not exist despite the implicit indications of the message >(such as a signature with a realistic name, including a phone number, etc.)

He notes that pseudoanonymous postings are active deception, rather than passive concealment of identity, and points out that he could set up a pseudonymous account for the purpose of fooling people into thinking that the pseudonym was a different person. Pardon me, but what on earth does this have to do with RISKS? The practice of publishing under a pseudonym has been common for centuries; ironically, Detweiler himself quotes "Shakespeare", believed by many to be a pseudonym.

He does on to hypothesize that people might be less wary of pseudonymous identities they don't recognize than they are of anonymous ones; he talks of megalomaniacs stalking the net. Well, if I see someone post to the net under a name I don't recognize -- like (say) L. Detweiler -- then I assign that person (whom I don't know) exactly the same probability of being a megalomaniac as I assign an anonymous user I don't know. Perhaps even a higher probability, as what megalomaniac would wish to remain *anonymous*?

Detweiler then points out that a user could post messages under a pseudonym, complimenting himself. Again, this is nothing new. Authors have been known to review their own books, written under pseudonyms; or to write letters to newspapers criticizing themselves.

Detweiler claims that public use of pseudonyms is often "dishonest, immoral, and unethical"; he demands that "others should be informed if it is occurring". Well, I hereby inform everyone that it is occurring, and has occurred for centuries, and will carry on occurring. It is not a new risk brought in by technology.

Perhaps the problem is that people have got used to the Internet being restricted to institutionalized settings, where user accounts are numbered, and verified to be unique by some central authority. As the Internet spreads into the real world, so the real-world practice of pseudonymity will inevitably spread into the Internet. When everyone has a computer, everyone can have a pseudonym; just as anyone with a pen and paper can develop a real-world pseudonym.

Detweiler next moves on to consider the use of pseudonyms in private communication. This, again, is nothing new. Look at the "Henry Root" letters (or "The Lazlo Letters"), Victor Lewis-Smith's crank phone calls, or any of thousands of similar examples. He complains that digital signatures do not solve the problem; unfortunately, he seems to be under the mistaken impression that written signatures are better. In fact, it is quite possible for a person to have multiple handwritten signatures.

Then, he moves on to what he calls the "dangerous, insideous [sic], and treacherous" uses of pseudonyms. He gives an example of an anarchist organization using pseudonyms to aid the destabilization of governments, democracy, law enforcement, and so on. Every good conspiracy must have a secret enemy trying to destroy the world. He speaks of carefully-guarded mailing lists and secret societies, and explains that the anarchists could send spoof communications to public addresses, magazines, and the like.

I hate to sound repetitive, but again, this threat is nothing new. Look at the spoof "LSD tattoo" announcements purporting to come from police officers, or the pranks played against government departments. Consider campaigners who write multiple letters under pseudonyms to send to politicians.

Detweiler then goes even further, talking about "pseudospoofers" as using "brainwashing and an illusion of peer pressure to manipulate unknowing

subscribers", with campaigns of "mental assault" to attack doubters. Of course, sinister mind-control techniques are a classic part of any conspiracy theory.

Next comes the masterstroke. He explains that the secret pseudospoofer cabal would attack people like him by "disparaging, discouraging and discrediting them publicly and privately as 'paranoid ranters' and 'conspiracy theorists'". So now anyone who criticizes his position is instantly One Of Them, a venomous snake who cannot be trusted, and further evidence of the Great Conspiracy. He suggests that they "might even be able to make a real-world pariah from simulated ire and criticism directed at a single strong opponent, say, L. Detweiler, from many simulated identities in cyberspace". Thus, he hopes, everyone who replies to RISKS criticizing his bizarre fears will become another piece of evidence in his favour.

He finishes off by suggesting that the evil pseudospoofers might already be infiltrating public mailing lists, discussion lists concerning email and security software, network administrators' mailing lists, CERT, the DNS databases, and so on. He likens pseudospoofing to a virus infecting the Internet. Again, like most conspiracy theories, the picture painted is one of an insidious threat which has already subverted our most cherished institutions!

I'm sorry if this seems impolite, but the entire article seems to me to be 10% misconceptions and 90% pure conspiracy theory. (Oh no! Mathew is One Of Them!) I find such things amusing, but I for one would appreciate it if this sort of nonsense was kept out of RISKS in future.

mathew

★ Re: Pseudospoofing (RISKS-15.25)

Alex Glockner <glockner@cosc.bsu.umd.edu> Thu, 11 Nov 93 14:37:22 EST

While I should be grateful to L. Detweiler for reminding us of the possibility of pseudospoofing on the Internet (sidenote: his anonymity FAQ makes for great reading...), we should also remember that this is 'just another' case of network problems that have always existed 'out there in the real world'.

The RTC (the US-sponsored agency that is responsible for selling off assets of failed Savings and Loan institutions) recently sold a beachfront property to the Audubon Society, a large US environmental group, which in cooperation with a developer would create a preserve from the property.

Whoops. Turns out it wasn't the environmental group -- officially, the National Audubon Society incorporated in New York State -- but a group, allegedly associated with the original failed developer, that chose to register in another state with the name "Audubon Society".

If the allegation is correct, the developer saved a lot of money from the original purchase price this way...

(My apologies for the lack of a citation; this appeared in the Washington Post in October 1993)

|> ... These are related to the potential of waging a systematic campaign of |> propaganda, disinformation, or brainwashing unleashed on an unsuspecting |> public by a subversive organization.

In American politics, we call this 'lobbying'. Any number of groups are misleadingly named and directed to achieve an agenda (*which* groups, of course, depend on your own beliefs, so I won't try to name any).

The fact is that most (all?) states have rules that you can choose any name (or more to the point, *names*) that you want as long as 1) the state cannot prove that it is in the public interest to deny your name change or 2) you are not intending to defraud anyone or escape legal obligations. Stage names and pen names are also long-established instances of this, also.

Pseudospoofing isn't anything new; it's just a new guise of something thousands of years old...what's the first C program everybody writes? "hello, world"? :-)

Alexander Glockner, Asst. Professor, Dept. of Computer Science, Bowie State University Bowie MD 20715 (301) 464-6609 glockner@cosc.bsu.umd.edu

★ The Perils of Pseudospoofing (Detweiler, RISKS-15.25)

Perry E. Metzger <pmetzger@lehman.com> Thu, 11 Nov 93 20:36:23 EST

I was amused to see that the article contained an elaborate, and amusingly paranoid, scenario, that describes, thinly veiled, the way that Mr. Detweiler apparently thinks that the "Cypherpunks" mailing list operates.

"Cypherpunks" is an informal group of privacy and cryptography advocates -the lists members include such varied individuals as Phil Zimmerman (the
author of PGP), Mike Godwin of EFF, John Gilmore, Phil Karn, a gentleman from
CPSR who's name I forget, and other fairly illustrious crusaders for privacy
and personal data security in the digital age.

Some members of the list are radical libertarians such as myself, who often point out (with some glee) that cryptographic techniques, which are essentially unstoppable because even high school students can now implement extremely secure cipher systems, will likely ultimately eliminate the capacity of the government and others to nose in where they do not belong.

With this introduction, I will explain what has happened: Mr. Detweiler has apparently decided that many members of the group are in fact the same person (posting under multiple identities) and that the entire mailing list is a monstrous plot to undermine Truth, Justice, and The American Way.

The allegation that most of the mailing lists members are identical is bizarre

-- anyone is free to check for themselves that people like Tim May, Eric Hughes, and others are real people. However, Mr. Detweiler became convinced that because so many people disliked his rantings on the list that they all had to, in fact, be the same person. I suppose the notion that more than one person might disagree with him did not cross his mind. I am not a qualified psychiatrist and do not pretend to be one, but I do know paranoid delusions when I see them.

As an example:

>The CryptoAnarchists might even be able to make a real-world pariah from >simulated ire and criticism directed at a single strong opponent, ...

I suppose it never occurred to Mr. Detweiler that he could simply look up folks like Eric Hughes (whom I believe lives in Berkeley), Tim May (whom I believe lives in Aptos, CA), and others, and verify that they exist and have differing voices and the like.

However, people who are suffering from insane fantasies rarely bother to listen if people tell them that they have insane fantasies.

The following paragraph speaks for itself:

>In fact, the CryptoAnarchists might even infiltrate sensitive internal mailing >lists like those maintained by CERT (Computer Emergency Response Team). ...

Perry Metzger

Personal Singularity

Jamie Dinkelacker <jamie@netcom.com> Thu, 11 Nov 1993 01:45:05 -0800

In a recent Cypherpunk post, the venerated individual E.Hughes suggested individuals make themselves known, and mention L.Detweiler's amorphous post to .risks. First, I'm honored to be mentioned along with May, Szabo, Finney, Hughes, ... indeed, fine company these electrons keep!

Jamie Dinkelacker is in fact and in blood an independent individual, living in Silicon Valley, who is finding profit from all the attention he's getting. He goes so far as to post his phone number for people who would care to call and offer consulting contracts for marketing management in the Bay Area.

More to the point: Jamie Dinkelacker is the only name I've used posting on the net.

Does Detweiler truly exist as an individual? Can anyone attest to his existence as separate from S.Boxx, Jim Riverman, David Sternlight? Who'll take a stand on his behalf?

Jamie Dinkelacker Palo Alto CA Jamie@netcom.com 415.941.4782

"L. Detweiler"'s single personality problem

Arthur Abraham <a2@ah.com> Thu, 11 Nov 93 15:14:39 -0800

I would like to attest from personal knowledge that the following personalities each emanate from a separate flesh and blood person:

G.Broiles, A.Chandler, J.Dinkelacker, H.Finney, E.Hughes, M.Landry, T.C.May, N.Szabo

I myself emanate from yet another flesh and blood person.

I have communicated with "L. Detweiler" in the past, and have frequently been amazed by his postings. His/her decline in the past month or two has been somewhat disturbing. It seems to illustrate how it is occasionally possible for strongly held positions, that seem to rely on an slightly unbalanced view of the world, to actually originate in unbalanced minds.

★ Re: pseudospoofing (RISKS-15.25)

leppik peter <leppik@uxa.cso.uiuc.edu> 15 Nov 1993 20:27:55 GMT

IMHO, I fail to see the real "risk" in pseudospoofing. Keep in mind that such famous people as Mark Twain and Marilyn Monroe never actually existed (they were "pseudospoofed," as it were, by Samuel Clemens, and Norma Jean, respectively).

The only possible risk that exists is if people lose their perspective, and forget the distinction between the network and the real world. Beyond that, the use of realistic-sounding nom-de-plumes for various reasons is a long and time-honored tradition. I see no reason why it should stop merely because the medium has become modulated electric fields, rather than ink and paper.

(Did William Shakespeare really exist? Some people with nothing better to do still argue about this question....)

Peter Leppik-- p-leppi@uiuc.edu

If people have a hard time understanding General Relativity, what makes us think computers will do any better?

★ Re: Snakes of Medusa and Cyberspace (RISKS-15.25)

<mc/G=Brad/S=Hicks/OU1=0205925@mhs.attmail.com> 15 Nov 93 21:11:08 GMT

"If your best friend jumped off of a cliff, would you? Did your mother ask you this? Every four years, lemmings jump off of cliffs. There are no five-year-old lemmings ... unless they've learned to think for themselves."

- recent TV ad for radio KPNT 105.7 FM, St. Genevieve/St. Louis, MO

OK, by now everybody knows that the lemmings story is a fake, but it's still a potent metaphor, and a relevant one to any discussion of what Mr. L. Deitweiler has termed "pseudospoofing." (Does Mr. Deitweiler exist? In my experience, most real people have first names.)

For those of you who've just subscribed, "pseudospoofing" is the use of "spoofed" SMTP mail connections, multiple anonymous mail servers, or other techniques to enable one person to send e-mail messages appearing to be from multiple people.

And if you missed Mr. Deitweiler's previous jeremiads, you might not know that this idea scares the water out of him. For example, consider this paragraph from the introduction to his latest lengthy posting on the subject, this one on RISKS Forum Digest, volume 15 issue 25, 10 Nov 1993:

- > ... These are related to the potential of waging a systematic campaign > of propaganda, disinformation, or brainwashing unleashed on an
- > unsuspecting public by a subversive organization.

Propaganda? I'll answer to that charge myself; I write propaganda for a small not-for-profit educational organization ... if you'll allow me to define propaganda as anything intended to influence people's opinions. (When I do it, it's a forceful essay. When you do it, it's called spin doctoring. When somebody we both think is "evil" does it, it's called propaganda.)

But the warnings of disinformation and brainwashing are something else altogether. Not for nothing did David Brin in his novel _Earth_ refer to a UseNet-like system as "the Net of a million lies." All manner of lies have appeared on the Net, from the US government's facile attempt to persuade us that Clipper is a harmless alternative to existing systems and won't be mandatory, to a recent (wonderfully funny) hoax having to do with modem taxes, that fooled even net veterans like Pat Townson of Telecom Digest.

But does pseudospoofing make it easier to lie successfully via the Net?

If I post a message here that says that I've met J. R. "Bob" Dobbs, and he really exists, will you believe me? Of course not; you know that I don't live in Dallas. (weak grin) You also know, by now, that J. R. "Bob" Dobbs is a myth built around a piece of 1950s clip art, and exists only in the same mystical realm as Santa Claus, Lazarus Long, the Easter Bunny, the World-Wide Satanic Conspiracy, John Galt, the Risen Lord Jesus Christ, the Tooth Fairy, and Wise and Benevolent Government. And you're not going to change your mind on the existence or non-existence of any of these things just because I, or anybody on the Net, told you otherwise.

Would you change your mind if ten people on the Net told you so? A hundred? A thousand?

Mr. Deitweiler has written that if I were to create (let us say) a hundred and twenty three alternate (fake) net.identities, and each of them sent him mail

telling him that black was really white, that he would be in imminent danger of dying at the next zebra crossing. He calls this process "brainwashing."

To compare pseudospoofed argumentation to brainwashing is to show that you are far, far too susceptible to peer pressure, and also to irresponsibly diminish the seriousness of brainwashing.

As Wilson documented in Leary's _Neuropolitics_, there is a technology for breaking down a person's resistance to ideas and lifestyles that are foreign to them, and "re-imprinting" them with the ideas and values of a new group. But among other things, it requires control of a person's physical environment, food, movement, social environment, and all punishments and rewards. Not for nothing do cult leaders take their converts to remote retreats, "deprogrammers" tie their captives to chairs in remote hotel rooms, fundamentalist preachers preach "separation from the world," and the military isolate recruits from all outside contact, control their every waking moment, and bully them mercilessly during the early weeks of boot camp.

But you cannot exert that kind of control over anyone's life or body or mind via the Net. All you can do is create fake peer pressure. And if you're that susceptible to peer pressure, Gods' pity on you. You need to learn to judge arguments by their quality, not by the number of people who say that they agree with them.

Does pseudospoofing have dire implications for democracy?

Well, no, because in the political context, pseudospoofing isn't that different from what interest groups do now. Do you really think that, for example, everybody who joins the AARP to get the club discounts agrees with everything that organization's lobbyists tell Congress? I doubt it, and any Congressman with any sense doubts it, too. What's more, with the rise of 800-number generated automatic telegrams, clipped coupons, and so forth, a new term has entered American political discourse, the term "astroturf campaign" -- that is, a fake grass roots campaign.

Sure, pseudospoofing provides another way to create a fake grass roots campaign. But will anybody be fooled? No. Congressional staff already look for close similarities between supporting messages and inform their bosses of them.

Somebody with enough determination could hand-write a thousand letters to Congress trying to influence a piece of legislation, carefully varying each one so that they look like they came from separate constituents. Without pseudospoofing, they would put them in separate envelopes and drop them in mailboxes all over the city over a course of days. With pseudospoofing, they could write a program to batch them out to anon mail servers or spoof them into SMTP mailers over the course of many days. But either way, the =real= work would not be in the mailing process, but in the laborious task of hand-writing a thousand entries while keeping them all different. Who is capable of such an effort?

Now, after thinking about the arguments above, if you are still terrified of the possibilities of pseudospoofing, take this challenge: try to design a

system that allows anonymous email and anonymous transactions that =doesn't= permit pseudospoofing. Such a system, it seems to me, will have to have =some= entity that knows which aliases go with which real.people, and such a system is by definition not anonymous.

After a hundred-plus lines, I am not going to go into the arguments about whether or not anonymity is itself a good or a bad thing. Suffice it to say that there are people, not involved in plotting the overthrow of society or any of Mr. Deitweiler's other paranoid fancies, who believe that anonymity is valuable.

All that I hope that I hope to accomplish with this message is to persuade you of is that there is little basis for fear that "the treacherous and toxic effects of pseudospoofing" will lead to "brainwashing" or "general destabilization of governments, democracy, laws, and law enforcement."

J. Brad Hicks Internet: mc!Brad_Hicks@mhs.attmail.com
X.400: c=US admd=ATTMail prmd=MasterCard sn=Hicks gn=Brad

Conspiracy 101? (Detweiler, RISKS-15.27)

Neil McKellar <mckellar@cs.ualberta.ca> Mon, 15 Nov 1993 15:22:51 -0700

In his article, "The Snakes of Medusa and Cyberspace: Internet identity subversion", L. Detweiler outlines a variety of methods by which 'pseudospoofing' can be used to influence public opinion and research (at least on the Internet). Having read a fair share of spy fiction in my time, none of these methods comes as a surprise to me. :-) And all these methods can be used AGAINST the conspirators in his scenario.

Perhaps it's time to pull out my copy of "Schroedinger's Cat" by Robert Anton Wilson, and bone up on conspiracy theory. :-)

Neil McKellar (mckellar@cs.ualberta.ca)

"Just because you aren't paranoid, doesn't mean they aren't out to get you."

Re: Snakes of Medusa and Cyberspace...

Leonard Mignerey <MIGNEREY@cua.edu> Thu, 11 Nov 1993 14:39:20 -0500 (EST)

I fail to see the difference between electronic pseudospoofing and print media pen names. It to me that all of Mr. Detweilers arguments hold for that scenario as well. The problem is not in pseudospoofing as much as in an individual relying on a single medium as a source of information. Certainly in the "War of the Worlds" incident, Orsen Wells pseudospoofed a number of people into believing that the Martians and actually landed. This unhappy group of individuals relied solely on their radios (and a single channel at that) for their information.

If we are to dive so deeply into cyberspace that it becomes the total extent of our research on important issues, then I think the problem is not in the pseudospoofers but in the pseudospoofed.

Leonard J. Mignerey, The Catholic University of America, Washington, DC 20064 Director, Management Information Systems INTERNET: mignerey@cua.edu

Pseudospoofing (ld, RISKS-15.25)

"L. Detweiler" <ld231782@longs.lance.colostate.edu> Sun, 14 Nov 93 19:57:16 -0700

Many people have emailed me to say that they are skeptical of my scenario about the Internet CryptoAnarchist pseudospoofing conspiracy published in RISKS-15.25. The scenario was built painstakingly from hundreds of messages I have reviewed on the subject over many weeks. I would like to present some of the more interesting pieces of 'evidence' (but withhold the more substantial pieces) that there is at least, in one quarter of the Internet, a very strong, systematic, and dedicated attempt to pseudospoof, and a very concerted effort, possibly, to cover it up and viciously attack those who seek to expose it.

My informal poll of pseudospoofing posted to the cypherpunks mailing list and talk.politics.crypto was unanswered by top Cypherpunk leadership, and many poll responses were very evasive, and several in the form `yeah, I have done it' with little additional information. The Cypherpunk mailing list and my private mail were my greatest source of inspirations for `Medusa's Snakes in Cyberspace'. For example, three prominent cypherpunks have suggested to me that there is a secret mailing list for `project development' free of `paranoid ranters'. I asked a cyperpunk leader about the existence of the list, and he said that `your question does not allow anything other than an incriminating answer.'

* * *

Here is a paragraph from a posting on the Cypherpunks list on Oct. 18 1993:

"In my limited experience creating Internet pseudonyms, I've been quite distracted by the continual need to avoid leaving pointers to my True Name lying around -- excess mail to/from my True Name, shared files, common peculiarities (e.g. misspellings in written text), traceable logins, etc. The penet.fi site explicitly maintains a list of pointers to the original address. All kinds of security controls -- crypto, access, information, inference -- have to be continually on my mind when using pseudonymous accounts. The hazards are everywhere. With our current tools it's practically impossible to maintain an active pseudonym for a long period of time against a sufficiently determined opponent, and quite a hassle to maintain even a modicum of decent security. Pointers to info and/or tools to enable the establishment and maintenance of a net.nym, beyond the standard cypherpunks PGP/remailer fare with which I'm now familiar, greatly appreciated. Especially nice would be a list of commercial net providers that allow pseudonymous accounts".

This paragraph contains an astounding amount of data on the possibility of a

highly refined, intense, extended, insidious, global, and systematic pseudospoofing effort. Some of the details it suggests, in particular:

- 1) Based on the context that surrounded this excerpt and the message, the author is intentionally conflating 'pseudonymity' (identification of the message implicitly indicates, 'this is a pseudonym', such as origination from anon.penet.fi) with 'pseudoanonymity' (the deception that 'I am a real person'). This is a classic cypherpunk tactic. I have hundreds of subtle variations of this obfuscation in my collection.
- 2) The author starts with 'in my limited experience in creating'... but clearly the author has *extensive* experience with meticulous practice and knowledge that rivals that of the most literate RISKS postings on the subject (for example, the anon.penet.fi site, the possibility of style analysis for identification, etc.)
- 3) The author clearly has an obsession to completely dissociating all traceability to his actual identity and a virtually fanatical aversion to 'pointers to my True Name lying around'. This includes extensive considerations for deleting mail, detecting shared files on a filesystem, and 'common peculiarities' like consistent misspellings.
- 4) The author refers to his efforts at deception as `security controls' and categorizes them in general categories of `crypto, access, information, inference' -- clearly he has dedicated an extreme amount of systematic thinking and effort to the `project' of pseudospoofing. He laments, sounding somewhat like an NSA administrator, that it's `quite a hassle to maintain even a modicum of decent security'.
- 5) There is an identifiable tone of paranoia in the message that most rational humans would not associate with casual anonymity. 'The hazards are everywhere'. The author laments, 'It's practically impossible to maintain an active pseudonym for a long period of time against a sufficiently determined opponent'.
- 6) The objective characterization of a 'sufficiently determined opponent' indicates the author considers attempts to trace the pseudoanonymity by what I have been calling 'demon exorcists' is an inevitable inconvenience that must be addressed. The author clearly considers it a routine hazard and has encountered and evaded it before. He considers his routine deceptions something like a game strategy.
- 7) Despite already obviously being an unsurpassed expert, the author requests 'pointers to info and/or tools to enable the establishment and maintenance of a ['pseudoanonym'], beyond the standard cypherpunks PGP/remailer far with which I'm now familiar, greatly appreciated.' This may also disguise an attempt to appear to be unsophisticated or determine what extent other 'octopuses' are existent in Cyberspace.
- 8) The author asks for a `list of commercial net providers that allow [pseudoanonymous] accounts' without regard to *geography* whatsoever, suggesting that it is no constraint. That is, the author may have no problem with accounts spread very wide geographically. This is in stark contrast to the standard request, `does anyone know a site in [x] area?' to avoid long

distance charges.

Clearly, the author has an *obsession* with maintaining *multiple*

`pseudoanonyms', possibly over a very *widespread* geographical area, has a
paranoia over exposure of one of his `tentacles' but also has conceived and
probably practiced countermeasures, and spends a great deal of time polishing
his techniques and arsenal. The author is not interested in casual anonymity
as a hobby. He is interested in systematic pseudospoofing, virtually as a
profession. He may even be spreading *disinformation* about his own
practices and the extent of his own knowledge. The author continues:

"Another big problem I see with [pseudoanonymous] reputations is entry. If most people are blocking posts from new pseudonyms, how does one get a new reputation established? I've had several years to establish a net.reputation for [...], and it might take a long time for any of my [pseudoanonyms] to catch up. Altruistic sponsorship requires trusted friends knowing the True Name, but that public sponsorship itself provides important clues to that Name."

This paragraph further promotes pseudospoofing, now suggesting its use in reputable forums:

- 1) Again, the author alludes to his arsenal of multiple pseudoanonyms, and expresses regret that it will take *a long time* of concerted pseudospoofing for before his other pseudoanonyms may `catch up'.
- 2) The author appears to be attempting to subvert mechanisms that bar pseudoanonymous identities, trampling on their right to do so in his obsessive promotion of the 'reputation' associated with his various name tags.
- 3) From the context of the message, and the references to `sponsorship by a true name', the author appears to actually be alluding to *identity databases* and ways of infiltrating them with pseudoanonyms. He laments that this `public sponsorship itself provides important clues pointing to that name.' This could be interpreted as a deliberate attempt at deception and corruption of a `True Name' database by conspiracy, and the `clues' that would `point' to a perpetrator of the crime.

Actually, because of the blurring of identities and misinformation this author promotes, I think that this paragraph may potentially be another disinformation stab -- the apparent owner of the message may be *itself* a pseudoanonymous identity, *itself* built up over `several years'! (The author posts from the site netcom.com, a site that is notorious for requiring essentially no proof of identity to receive an Internet account.)

The author continues with classic cypherpunk dogma that blurs pseudonymous and anonymous identities with pseudoanonymity ('pure anonymity'), and vilifies those who feel 'threatened' by the latter:

"I hope that we stick to experimenting with pure anonymity in many venues. I suggest we'll find out that purely anonymous vposts are not so bad, overall. [...] Pure anonymity is a strange, threatening, fascinating beast in our panoptic social-welfare world. Even those of us at the forefront of

harnessing this monster shrink back in fear when it whinnies. [...]"

Now, superimpose the 'Medusa's Snake's and Cyberspace' essay in your mind as you read the following:

"Pure anonymity provides a voice for a wide variety of new kinds of expression that up until now have been suppressed. [...] I hope we continue experimenting with pure anonymity for a while longer [...]. Some of what comes out might look very strange, something like tapping into previously concealed areas of our social psyche. I suspect the result will be a more honest dialog, a more productive conversation freed from posturing and, ironically, from the concealment of threatening truth. I hope we will observe with Zen patience and allow this quite interesting experiment to continue."

* * *

Since the above posting was to a public list, I will reveal the author of the message I have been dissecting. He is the same person who took my short comment at the end of the `Medusa's Snakes & Cyberspace' essay as an *accusation* that some pseudanonyms may be listed. He writes in RISKS-15.26:

>I'd like to assure the readers of RISKS that I am in fact a unique person,
>distinct from the other names L. Detweiler listed. Of the people on his list
>I know from personal contact, all are distinct people in Real Life(tm). Well
>before his post to RISKS, L. Detweiler was provided means of personally
>verifying that many of the names he listed are distinct True Names (eg phone
>numbers he can call), but it doesn't seem to help.

Let's dissect these statements with an eye to rigor. 'I am in fact a unique person [...]' means nothing in the question of pseudanonymity -- Medusa may have one of her Snakes claim that 'I am a unique person' without lying.

Next, 'Of the people on his list I know from personal contact, all are distinct people in Real Life(tm)'. But this can be taken to mean only that more than one person is represented by a list of pseudoanonyms. Note the author is careful not to mention *which* people he knows from personal contact. That, after all, might reveal 'important clues pointing to that Name'!

Also, there is a problem that members of a `cult of pseudospoofers', who subscribe to the `pseudoreligion of pseudoanonymity', as this person apparently does, may twist language to the point of actually maintaining that different pseudoanonymous identities *are* different `people', even when typed in at a keyboard by the same individual! This would not be unlike a fanatic religious sect maintaining that acts of `terrorism' are actually `holy liberation' when committed in the name of God!

The author says he is `distinct from the other names L. Detweiler listed.' But again, this is not a guarantee of uniqueness of flesh! The use of the word `name' instead of `people' is quite suspicious in our context! The whole *issue* is that beyond the uniqueness of mere ASCII `names'!

The person goes on to state that 'Well before his post to RISKS, L. Detweiler was provided means of personally verifying that many of the names he listed

are distinct True Names (eg phone numbers he can call) but it doesn't seem to help.'

The people I listed are separated by vast geography in their posting sites, with a concentration in California. Furthermore, I have been in private correspondence with all of them over many weeks, and I am unsure of what specifically Mr. Szabo is referring to as my opportunity to verify that `many of the names' are `distinct True Names'. I have never before posted a list of this set of names before! The lack of specific information is highly suspicious in our context! Furthermore, in our context, the issue would not be whether `some' real people are represented in the list, but whether *all* names listed correspond to the legal identities of *unique* human beings! (A complex and widespread pseudospoofing effort actively being orchestrated by some, which very possibly spans many states, may not even be thwarted by the necessity of establishing interstate telephone numbers!)

* * *

Finally, I have very strong tangential cues that the 'Medusa's Snakes in Cyberspace' essay is far more true than hypothetical. Over many weeks I have encountered strong stonewalling, evasion, and counterattacks from some of the most prominent cypherpunks in response to my specific allegations in email. This included a mailbombing, a mailbombing threat, four letters to my site postmaster, two from cypherpunk leaders, one referring to 'your latest paranoid descent into fantasy in RISKS', my 'violent threats', without quoting any of my statements in particular (I find the thought of a physical threat abhorrent), and suggested 'I have a strong feeling you are going to have a very hard time getting a job in the computer industry' in part from the essay. Another called my efforts against pseudospoofing a 'a nonsensical, paranoid, one-man jihad against cypherpunks'. Apparently because the lamentations and supplications to my postmaster have largely been ignored, one cypherpunk suggested that 'I intend to go beyond your postmaster on the next try, to various former classmates and old friends of mine who are computation center employees, faculty, and administration members at CSU now.'

Incidentally, there is a strong overlap between the people perpetrating the above activities and those I credited at the end of my essay. Elsewhere, one cypherpunk suggested that 'I better start looking over my shoulder'. Another, in what might be termed 'psychopunk humor,' wrote 'I'm going to come kill your family with a rusty razor blade' (the latter broadcast on the entire mailing list) and suggested it demonstrated my personal problems in being upset by such a message.

These tactics are all quite shocking to me, and I am not sure how to respond to these letters except to perceive them as outrageous and desperate attempts to intimidate and censor me indirectly where other approaches have failed. I warn others of the searing hostility they may encounter on the cypherpunks list -- with philosophies promoted there that are increasingly blurred with raw criminality -- and against any attempts to find an antidote to poisonous pseudospoofing.

L. Detweiler



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 28

Weds 17 November 1993

Contents

Power problems stops Milano Stock Exchange for 4 hours Lorenzo Strigini

Lawver discovers the RISK of computer efficiency

Martin Minow

Living Will Database

Brian Hawthorne

Review of "Second Contact" by Resnick

Rob Slade

UK government to scrap safety laws

Jonathan Bowen

Tablespoons, or, handwriting recognition may be hazardous to your poem.

Mark Brader

Visa introduces transaction UIDs

Bob Frankston

Re: CERT Reports and system breakins

Steve Bellovin

Re: MASS state police confusion

Eric N. Florack

Re: Ada Usage

Harry Erwin

James H. Haynes

Re: Groundhog Day, D-Day, Remembrance Day, and all that mathew

A Myth is as good as a Smile

Call-for-Papers for 17th Nat'l Computer Security Conference Louise Reiner

Info on RISKS (comp.risks)

✓ Power problems stops Milano Stock Exchange for 4 hours

Lorenzo Strigini <strigini@iei.pi.cnr.it> Wed, 17 Nov 93 09:13:26 MET

Yesterday, 16th of November, trading at the Milano Stock exchange started late at 14:30 because the "telematic" system was down due to a power failure "dating from the previous day" (I am quoting "II Sole 24 ore", "political economical-financial daily"). The day was bad for the market, with the "Mib" stock index going down 2%. This is attributed to political uncertainties coinciding with a normally bearish period of the year. A morning radio newscast, interviewed an "expert". Excerpts (from memory): the system is undergoing major changes as it will soon handle 100% of the trading vs 70% now (it was not clear whether by number of transactions, of stocks or by value); there is no reason for worry "as this was a hardware, not a software fault"; such problems are unavoidable, as "even satellites and space shuttles, with computers that are not duplicated but triplicated , have had their launches aborted due to such problems" (the interviewer sensibly asked "leave satellites alone and tell us about stock exchanges", and the interviewee said that comparable failures have occurred at the London, Paris, New York exchanges. I have no information about the stated availability requirements, the architecture of the system, and the provisions for recovery (if others have such information, I'd appreciate it if they mailed it to me).

Lorenzo Strigini IEI-CNR Via Santa Maria 46 I-56126 Pisa - Italy tel. +39 50 593495; fax +39 50 554342 E-mail: strigini@iei.pi.cnr.it

Lawyer discovers the RISK of computer efficiency

Martin Minow <minow@apple.com> Tue, 16 Nov 93 17:09:40 -0800

>From the New York Times, Friday November 12, 1993 (page B20):

At the Bar. David Margolick. "Court asks a lawyer, if a computer is doing most of the work, why the big fee?"

[Abstracted and excerpted] Craig Collins, a lawyer in San Mateo California, used the West CD-ROM library, a system that contains every court opinion published in California in the last 33 years on three compact disks, to research a parental rights case. Under penalty of perjury, he swore that he had devoted 22 hours, ten of them over the Fourth of July weekend, to writing several memorandums concerning the rights of step-parents in custody cases. "At his normal rate of \$225 an hour, that worked out to \$4,950, part of his total tab of \$9,591.50. The money was to come from the stepfather, who lost the case, provided it was approved by Judge Roderic Duncan of the Alameda County Superior Court."

"That was not quite what happened. Indeed, after deconstructing the mechanics of modern computer research, Judge Duncan not only balked, but handed Mr. Collins to the disciplinary enforcement section of the State Bar of California."

As it turned out, large portions of Mr. Collins memorandums were copied directly from the court opinions, without attribution. Collins explained that he had quoted the courts at length because "their language "was better written than I would have composed it myself." The court, however,

found that 22 hours was rather extreme for cutting and pasting since Mr. Collins was an experienced lawyer. At the hearing, William P. Eppes II, a representative of the West Publishing Company testified that Mr. Collins had used the system for a total of of 9 hours and 33 minutes since he had purchased it. The witness, who was also a lawyer, testified that it seemed entirely plausible that Mr. Collins had put in the time he claimed.

The judge was impressed by the witness' reasoning and withdrew his claim that Mr. Collins had not worked as long as he did. "All those hours at the computer, the judge seemed to say, reflected inefficiency rather than dishonesty."

Although disciplinary proceedings were dropped, Mr. Collins is still displeased with a judge who, in an interview, he described as "a ``cavalier'' judicial ``maveric'' whose ill-considered opinions had periodically been criticized by the California courts of appeal. How did he know? He consulted his trusty CD-ROM, and plugged in the words ``Duncan'' and ``reversal.''''

["Quotes" are directly from the article. ``Quotes' are quoted material in the original article.

On the same page of the Times, you will also find an interesting article on modern computerized fingerprint systems. The FBI has a database of 30 million unique cards and performs more than 32,000 searches per day. The modern systems can compare a print at rates faster than 1,000 per second.

Martin Minow minow@apple.com]

Living Will Database

Brian Hawthorne - SunSelect <Brian.Hawthorne@east.sun.com> Mon, 15 Nov 1993 10:20:26 +0500

A recent item on the New York Times newswire described a patent granted to Victor Alan Perry (date: 11-14-93 1811EST/category: Financial/ subject: BC PATENTS/title: PATENTS: FAT SUBSTITUTE COULD BURN UP; LIVING WILL DATABASE/author: TERESA RIORDAN).

Apparently, Mr. Perry, et alia, have been granted US patent 5,241,466 for a "system for administering a central depository for living wills". He envisions an '800' number that doctors and hospitals can call. The system will then fax back a copy of the appropriate document (living will, durable power of attorney, etc.) for the patient. He would also like to extend the system to be modem-accessible.

The purpose of the system is to save some of \$10,000,000,000 which is claimed to be spent "for artificial life support of people who did not wish to be kept alive".

[That would make an interesting target for computer break-ins! PGN]

"Second Contact" by Resnick

"Rob Slade, Ed. DECrypt & ComNet, VARUG rep" <roberts@decus.arc.ab.ca> 13 Nov 93 19:46 -0600

BK2NDCNT.RVW 931014

Tor Books
49 West 24th Street
New York, NY 10010
"Second Contact", Resnick, 1990, U\$3.95/C\$4.95

The jacket blurb states that this book is a treat for anyone who likes "computers, science fiction, or just a plain good read." The "good read" part is going to depend on personal preference: the science fiction part seems to be almost a side issue. The computer enthusiasts will be presented alternately with ideas and giggles.

The book is set seventy-five years into the future. Neither politics nor technology appears to have advanced very far and, with a publication date just before the "Seven Days That Shook the World" (as CNN would have it), the major national security concern of the US is still "Russian spies". (Interestingly, the book lists the US, Russia, China and Brazil as spacefaring nations, while the cover shows a clear shot of a "NASA/ESA" logo on a rocket-like device.) Computers equipped with voice recognition still cannot deal with more than one speaker. At one point a computer retailer tells one character that if the modem (what happened to ISDN?) she is trying isn't fast enough, they have one that will transmit at "38,400 baud." (If the author isn't just confusing baud and "bits per second" this indicates some improvement over "voice grade" lines, but hardly enough for the seemingly ubiquitous "vidphones" unless trellis coding has gotten *really* sophisticated.)

None of the data security or communication issues raised are terribly sophisticated. The author has apparently never heard of telnet capabilities or the like. As usual in fictional accounts, the "hacker" is not only skilled with computers, but is a phone phreak as well.

Two of the security topics are of some interest. One is the account of files being secured by "moving". The concept of "security by obscurity" is justifiably condemned, but it is true that leaving "standard" accounts open or having "standard" directory and file structures is, to a certain extent, a potential security loophole. The next logical step, beyond putting files in a non-standard location, is to keep moving the files. Unfortunately, there must be a way to retrieve the files, so somewhere there must be a pointer to them.

The other point regards database security. At one stage of the plot, the heroes are trying to track the identity of an individual who is "classified to the max." By using the database inference problem, they are able to pinpoint his location. The example is somewhat simplistic, but involves generating a number of queries and discarding the ones the computer does *not* reject as classified.

The topic of alien contact, suggested by the title, is really of relatively minor importance. A computer security whimsy in sf clothing.

DECUS Canada Communications, Desktop, Education and Security group newsletters Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733 DECUS Symposium '94, Vancouver, BC, Mar 1-3, 1994, contact: rulag@decus.ca

UK government to scrap safety laws

<Jonathan.Bowen@prg.ox.ac.uk>
Mon, 15 Nov 93 09:36:30 GMT

The following is extracted from the lead article on the front page of the 14 November 1993 issue of The Independent on Sunday:

"A RAFT of safety legislation will be scrapped in a Bill that the Government is to announce this week in the name of minimising costs to commerce and industry. It will be the biggest shake-up of health and safety law in 20 years. ...

One element will be the abandonment of the longstanding assumption that safety legislation can only be repealed if it is replaced by regulations just as tough. ...

Michael Heseltine, President of the Board of Trade, also wants to revoke European regulations safeguarding millions of people who work with computer screens. He plans to play down the risk of repetitive strain injury and abolish the requirement on employers to provide eye tests and glasses if they are needed."

As is typical in the UK, details were leaked to the press ahead of the planned Deregulation Bill to be announced in the forthcoming Queen's Speech to Parliament.

Jonathan Bowen, Oxford University

[Might that imply the demise of DEFSTAN 00-55 and 00-56? PGN]

Tablespoons, or, handwriting recognition may be hazardous to your poem

<msb@sq.com> Wed, 17 Nov 1993 13:35:18 -0500

[This poem was generated by entering Lewis Carroll's poem "Jabberwocky", from "Through The Looking Glass" into an Apple Newton. Nonsense words in the original were each written three times to get the most consistent match.]

TABLESPOONS

Teas Willis, and the sticky tours Did gym and Gibbs in the wake. All mimes were the borrowers, And the moderate Belgrade. "Beware the tablespoon my son, The teeth that bite, the Claus that catch. Beware the Subjects bird, and shred The serious Bandwidth!" He took his Verbal sword in hand: Long time the monitors fog he sought, So rested he by the Tumbled tree, And stood a while in thought. And as in selfish thought he stood, The tablespoon, with eyes of Flame, Came stifling through the trigger wood, And troubled as it came! One, two! One, two! And through and though, The Verbal blade went thicker shade. He left it dead, and with its head, He went gambling back. "And host Thai slash the tablespoon? Come to my arms my bearish boy. Oh various day! Cartoon! Cathay!" He charted in his joy. Teas Willis, and the sticky tours Did gym and Gibbs in the wake. All mimes were the borrowers,

Lewis Carrol's JABBERWOCKY as "recognized" by the Apple Newton, (c) 1993 Robert McNally. Permission is granted to reproduce this if the copyright remains intact.

["It seems very pretty," she said when she had finished it, "but it's rather hard to understand!" (You see she didn't like to confess even to herself, that she couldn't make it out at all.) --Lewis Carroll]

Forwarded to rec.humor.funny and comp.risks by Mark Brader

Visa introduces transaction UIDs

And the moderate Belgrade.

<Bob_Frankston@frankston.com> Sun, 14 Nov 1993 16:07 -0400

There is an article in The New York Times of 14 Nov 1993, Page F9, about how Visa is (finally!!!) introducing transaction-unique IDs into its system as a way of tracking transactions and, of course, reducing fraud. They also use the term "digital signature", but, I presume, they are simply corrupting a technical term by misappropriating it for another function. They seem to mean "unique ID", but perhaps they are also worried about spoofed transactions. Can someone provide more information on this?

Re: CERT Reports and system breakins (Karn, RISKS-15.22)

<smb@research.att.com>
Mon, 15 Nov 93 11:41:38 EST

We need strong security mechanisms based on good cryptography and well thought out protocols. They're underway, but they will take time to develop.

In <u>RISKS-15.22</u>, Phil Karn suggests that the major network security issue is the lack of good protocols. While that's certainly a problem, I don't think cryptographic authentication will do that much to solve the network security problem.

Cryptography does two things: it provides secrecy if you want it, it it provides authentication, either explicitly or implicitly, since a packet encrypted with the wrong key will decipher to garbage. Both will help somewhat; properly-targeted encryption will eliminate password-sniffing, and cryptographic authentication will allow more hosts to extend trust to users or other hosts on a more rational basis.

However, cryptography does nothing to solve the *host* security problem. My incoming mail traffic could be protected by triple DES composed with quadruple IDEA -- and it will do me no good if the mailer has bugs in its implementation of good old RFC821 and RFC822. Nor will Kerberos and my one-time password help against an opponent who has sabotaged my shell, so that he or she will get back-door access to my account and my cryptographic credentials. After all, the privileges that let intruders monitor Ethernets and install boobytrapped login and telnet commands will let them change anything else on my system. Fixing network protocols will do nothing to guard against buggy specifications or buggy implementations.

The real issue is one of software engineering. At the last USENIX UNIX Security Conference, Robert H. Morris gave the keynote address. Its title was on the order of ``If your software is full of bugs, what does that say about its security?" That's the real issue -- learning how to get *host* security right.

--Steve Bellovin

★ Re: MASS state police confusion (Garfinkel, RISKS-15.26)

<Eric_N._Florack.cru-mc@xerox.com>
Mon, 15 Nov 1993 07:08:40 PST

<>"It wasn't actually a tape of vehicle owners. They got stickers confused with people who were supposed to get food stamps. So the people [who were supposed to get] the food stamp books got the gun permits, and the people who were supposed to get gun permits got food stamps. But it wasn't the Registry this time."<<

Gee, I know /I/ feel better, now.... NOT!!!!!

I mean, we're not supposed to be concerned that gun permits were issued to food-stamp recipients.... a group that has been traditionally prone to living

in high-crime areas? As much as I'm against gun control, issuing permits to untested people would seem to present a very clear RISK.

His screams of 'It's not our fault /this time/' suggests that there is a bit of history, here, for this kind of error. Gee, I feel REAL secure, knowing our all powerful, and deeply caring government is so able and willing to help us.

And there's a big government type in the Kremli..(ahem) WHite House? (Sh-sh-sh-shudder)

Be afraid., Be very, very afraid.

Eric Florack.CRU-MC@Xerox.COM

Re: Ada Usage

Harry Erwin <erwin@trwacs.fp.trw.com> 15 Nov 1993 16:04:38 GMT

There are real problems for which Ada is not the best language.

- 1. Simulation--due to the lack of support for coroutines, Simula-style semaphores, condition queues, call by name, and event lists,
- 2. Test generation--for similar reasons,
- 3. Multi-threaded applications with external inputs, where the usual tasking libraries run into problems. What happens is that the OS and the run-time environment sometimes need to enter messages or events into the same queues. Unless the library has been carefully integrated with the operating system, race conditions can occur, losing entries.
- 4. Object-oriented programming in the full sense,
- 5. Completion routines for inter-device protocols, and
- 6. Anything that needs to run close to the bare metal.

Cheers,

Harry Erwin erwin@trwacs.fp.trw.com herwin@cs.gmu.edu Working on Freeman nets.

★ Re: No change in Ada policy (anonymous, RISKS-15.26)

James H. Haynes <haynes@cats.ucsc.edu> 15 Nov 1993 21:46:41 GMT

>If the government really believes in capitalism, and if the government >believes that private industry is in business to make money, then the >government should be willing to allow industry to transition to Ada as that >makes economic good sense. And not sooner.

But the defense business is a very peculiar flavor of capitalism. The defense companies may see it as being in their own best interests to program in company-proprietary languages forever. I believe this was

part of the justification for Ada.

haynes@cats.ucsc.edu haynes@cats.bitnet

David Brin ==> Vernor Vinge (minor correction) (Hicks, RISKS-15.27)

the person your mother warned you about <phydeaux@med.cornell.edu> Tue, 16 Nov 1993 13:04:43 -0500

In RISKS-15.27, mc!Brad_Hicks@mhs.attmail.com wrote:

>altogether. Not for nothing did David Brin in his novel _Earth_ refer to a >UseNet-like system as "the Net of a million lies." All manner of lies have

Only one thing, of course, is that the "Net of a Million Lies" comes from Vernor Vinge's "A Fire Upon the Deep," rather than Brin's Earth.

Doesn't really change the validity of the argument however.

How is this correction relevant, you ask? Because any piece of wrong information, no matter how slight, is at risk of being spread throughout the world!

73 de Dave Weingart KB2CWF phydeaux@cumc.cornell.edu (212) 746-3638

★ Re: Groundhog Day, D-Day, Remembrance Day, and all that (RISKS-15.25)

mathew <mathew@mantis.co.uk> 11 Nov 1993 12:13:34 -0000

msb@sq.com writes:

>And one day early this month, *I* learned that it's also a good idea >to test a program both during and after the first 9 days of the month. >Gotta watch those 1- and 2-digit numbers!

On a related note, a good date to try is the first 2-digit Wednesday in September, if your program produces English language output.

mathew

[Yes, I noted that very day in RISKS, the first time the masthead line went over 80 characters on that day, truncating the issue number! PGN]

A Myth is as good as a Smile

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 16 Nov 93 17:40:13 PST

I received a lot of out-of-band comments about L.Detweiler's piece in RISKS-15.25, and still more asking why I devoted a whole issue (RISKS-15.27)

to the responses. (I tend to do dedicated issues when I get an enormous flurry of follow-ups, so that if you do not appreciate the subject matter, you can disregard it in its entirety.) There were many suggestions that this topic should end immediately, which it will, I hope, with this message. But remember, folks, the lack of E-mail authenticity, message integrity, and personal accountability is a real potential problem throughout the Internet, not only on April Fools' Day.

Almost no one commented on the original title, Snakes of Medusa. Someone suggested that the Hydra might have been more appropriate, the serpent that started with nine heads and regenerated two to replace any one that was severed. There is a REAL multiple-identity problem. (Medusa was the snaky-haired Gorgon whose glance would turn you into stone. A cheesy biography of stoned individuals might been written by Gorgon Zola.)

At any rate, further follow-up messages from Eric Hughes and L.Detweiler can be found in the RISKS archive on CRVAX.SRI.COM in directory RISKS: under the file name <u>RISKS-15.28</u>X. That is the end of it in RISKS. For further discussion, try L.Detweiler or the Cypherpunks newsgroup.

Call-for-Papers for 17th Nat'l Computer Security Conference

<Reiner@DOCKMASTER.NCSC.MIL>
Mon, 15 Nov 93 10:15 EST

CALL FOR PAPERS & PANELS - 17TH NATIONAL COMPUTER SECURITY CONFERENCE
October 11-14, 1994 --- Baltimore, Maryland
Co-Sponsors: National Institute of Standards & Technology
National Computer Security Center

The National Computer Security Conference attendees represent a broad range of information security interests spanning government, industry, commercial, and academic communities. Papers and panel discussions typically cover:

- research & development for secure products and systems;
- implementation and accreditation of secure systems;
- administration & operation of secure systems;
- evaluation of products and systems against trust criteria;
- international harmonization of security criteria & evaluations;
- promotion of computer security: education, awareness and training;
- social and legal issues related to computer security.

We invite the submission of papers and proposals for panels in any of the above areas and on other topics related to the confidentiality, integrity, and availability of data and resources in information systems. Papers will be selected through an anonymous review process and will be published in the conference proceedings. Panels will be selected by the Program Committee, and panel members will be expected to provide written statements for inclusion in the proceedings.

BY 1 MARCH 1994: eight (8) copies of your paper or panel proposal

should ARRIVE at the following address:

National Computer Security Conference ATTN: NCS Conference Secretary, APS XI National Computer Security Center Fort George G. Meade, MD. 20755-6000

By 1 June, 1994: Authors and panel chairs selected to participate in the conference will be notified and advised when final papers and panel statements are due.

PREPARATION OF CONFERENCE SUBMISSIONS:

Cover sheet: Type of submission (paper, panel, tutorial)

Title or Topic

Abstract (not to exceed 250 words)

Author(s)

Organizational Affiliation(s)

Phone numbers (voice and fax if available)

Internet address if available

Point of contact if more than one author

SUBMISSIONS RELATED TO WORK UNDER U.S. GOVERNMENT SPONSORSHIP MUST ALSO INCLUDE THE FOLLOWING:

Program Sponsor or Procuring Element Contract Number (if applicable) Government Publication Release Authority

Paper preparation: 10-page maximum incl. figures & references; title, abstract, & keywords on first page; no more than 12 char./inch & 6 lines/inch; one-inch margins all around.

BECAUSE THE REVIEW PROCESS WILL BE ANONYMOUS, NAMES AND AFFILIATIONS OF AUTHORS SHOULD APPEAR ONLY ON THE SEPARATE COVER SHEET

CLASSIFIED MATERIAL OR TOPICS SHOULD NOT BE SUBMITTED

RELEASE FOR PUBLICATION & COPYRIGHT:

It is the responsibility of the authors to obtain government or corporate releases for publication. Written releases will be required for all papers to be published. Papers developed as part of official U.S. government duties may not be subject to copyright. Papers that are subject to copyright must be accompanied by written assignment to the NCS Conference Committee or written authorization for publication and release at the Committee's discretion.

PANEL PROPOSALS:

Panels should be geared to a maximum of ninety minutes long, including time for prepared remarks and audience interaction.

2 page maximum.

Include chair and proposed panelists or organizations to be

represented on first page.

Include summary of topic, issues, and/or questions to be addressed by the panel and viewpoints that proposed panelists would bring to the discussion.

FOR MORE INFORMATION ON SUBMISSIONS, PLEASE CALL 410-850-0272 OR SEND INTERNET MESSAGES TO: NCS_Conference at DOCKMASTER.NCSC.MIL.

For other information about the conference, call 301-975-2775.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 29

Tuesday 23 November 1993

Contents

Logic Bomb planted in retribution for nonpayment

Mich Kabay

Brazilian computer snarls in corruption probe

Mich Kabay

Digitized Photos

Mich Kabay

Magnetic Fields & Leukaemia

Mich Kabay

Who owns the unused cycles?

Bear Giles

Not-voting-by-phone Boulder over

Bear Giles

Tablespoons, or another risk?

Steve VanDevender

Charge cards from mail order houses

Ted Wobber

United Parcel Service signatures

Jim Carroll

Re: Massachusetts state police confusion

Brian Hawthorne

Re: Ada Usage

Douglas W. Jones

Robert I. Eachus

Re: UK government to scrap safety laws

Keith Lockstone

Info on RISKS (comp.risks)

✓ Logic Bomb planted in retribution for nonpayment

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 23 Nov 93 16:51:46 EST

Excerpted from the Associated Press Newswire via Executive News Service (GO ENS) on CompuServe:

APn 11/23 0106 BRF--Computer Virus

WESTBURY, N.Y. (AP) -- A computer company owner and his technician are accused of planting a virus in a dissatisfied customer's computer system, after the customer refused to pay for a program.

Michael Lofaro, 29, owner of MJL Design of Manhattan, and his technician, John Puzzo, 22, were charged Monday with attempted computer tampering and coercion, said Lt. Lawrence Mulvey of the Nassau County police.

The article explains that the maximum penalties are 4-7 years and up to \$5,000 in fines. The client, William Haberman, owner of Forecast Inc., a furniture company in Westbury, complained about poor performance in a program sold by MJL Design and refused to pay the full invoice when the vendor allegedly ignored his complaints.

According to the accusation, Lofaro and Puzzo planted a ``computer virus'' [which I think is simply a logic bomb, judging from the phrasing--MK] and threatened to detonate it.

The accused were arrested when they came to defuse the logic bomb.

[Surprising to see the old confusion between viruses and logic bombs persisting in a newswire report.--MK] [Not surprising at all.--PGN]

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

Brazilian computer snarls in corruption probe

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 23 Nov 93 16:52:01 EST

>Excerpted from the United Press International newswire via Executive News Service (GO ENS) on CompuServe:

UPn 11/18 1948 Data-packed computer snarls in Brazilian corruption probe

BRASILIA (UPI) -- A congressional committee investigating massive fraud in Brazil was held up Thursday when the computers froze in response to a command to cross-reference data on thousands of checks, bank accounts and budget amendments between 1990 and 1992.

The article explains that the network ran out of processing resources, including memory, when trying to track down corruption in the government.

[Wonder if we'd need a supercomputer to track corruption in certain other governments?--MK]

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

Digitized Photos

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 23 Nov 93 16:52:27 EST

>Excerpted from the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

APn 11/21 1531 Digital Licenses, By MARTIN FINUCANE, Associated Press Writer BOSTON (AP) -- Fourteen states and two Canadian provinces are planning to use digitized photographs of drivers on licenses, adding people's faces to their already-vast computer files.

Once a photo is scanned into a computer to be stored digitally, the image can easily be altered, matched with similar images or even transmitted around the world. Privacy experts worry that the information will be misused by people with bad intentions or by overzealous police.

The article goes on to explain that privacy advocates are already worried about the potential for abuse. Possible abuses include

o release of the pictures to the direct-marketing industry, which could target specific categories of people (e.g., bald people or those in need of dental care) for campaigns;

o illegal use by criminals to stalk, harass or intimidate victims.

The FBI is claimed to be interested in nationwide picture files and is currently upgrading its databases to handle pictures such as those from motor vehicle licenses.

Even in police work, such files could be misused: "For example, courts have frowned on police roundups of all young black men near a crime scene -- but police could use the computer to scan the pictures of every driver living in the area."

Police could greatly increase the number of pictures shown to witnesses of crimes by including thousands of photos of innocent people--with a likely increase in the number of false positive misidentifications.

Because the pictures will be stored in digital fashion, changing them will be very easy.

Privacy watchdogs urge caution and thought as the systems are implemented.

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

Magnetic Fields & Leukaemia

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 23 Nov 93 16:52:47 EST

>Excerpted from the Reuter newswire via Executive News Service (GO ENS) on

CompuServe:

RTw 11/18 1718 MAGNETIC FIELDS DOUBLE RISK OF CHILD LEUKAEMIA-RESEARCH

LONDON, Nov 19 (Reuter) - Children who live close to high voltage power lines and other electromagnetic fields may be doubling their risk of contracting leukaemia, according to research published on Friday.

An analysis of three of the latest studies carried out in Denmark, Finland and Sweden also threw up evidence of an increased risk of nervous system tumours and other childhood cancers, although the link was less clear.

The article goes on to explain that the analysis was published in a letter to The Lancet, a British medical journal. Unlike previous studies which were widely viewed as having insufficient sample sizes, "Anders Ahlborn of Stockholm's Institute of Environmental Medicine and his Nordic colleagues looked at recent Danish and Finnish studies that used the entire population and a Swedish study restricted to people living close to power lines."

[It will be interesting to see if the levels of electromagnetic disturbance from electronic equipment could affect us too.--MK]

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

Who owns the unused cycles?

Bear Giles <bear@tigger.cs.colorado.edu>
Wed. 17 Nov 1993 19:43:06 -0700

Earlier today I talked my sys-admin into letting me install the software to help factor RSA-129 on my workstation. When I mentioned how easily it installed he suggested I run it on a number of other workstations -- after all I had login permissions for them all.

An hour later a coworker was giving me a stern lecture about how I shouldn't run a process on his system in background without getting his full permission first (not only to run it and to be assured that it would not consume resources, but also that it satisfied *his* requirements for legitimacy). The fact that the process was nice'd and previously approved by the sys-admin was considered irrelevant.

I've since talked to several other coworkers; about 1/3 feel the same as the coworker mentioned above, the other 2/3 feel that if the system resources are available they can be used by anyone as long as they don't impact the primary user. *Everyone* appears to believe that their view is obvious, although most admit that other views are not totally unreasonable.

This specific application is trivial, but what does this portend for the future? It's not hard to identify legitimate background tasks which could be run by businesses overnight, but will efforts to use idle resources run into hostility by workers who feel that ``their'' workstation or PC is being grabbed by others who don't respect their privacy or ownership? Would such

distributed software be acceptable at night, or by users without any indication of system load (be it ``perf meters" or flashing disk lights), but not by users who could notice such indications of active processing?

Distributed processing over LANs seems promising, but have users had individual PCs and workstations which acted alone too long for them to accept the idea of a supra-system computer?

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

✓ Not-voting-by-phone Boulder over

Bear Giles <bear@tigger.cs.colorado.edu>
Thu, 18 Nov 1993 21:27:06 -0700

During the recent elections the people of Boulder, Colorado voted 11731 to 7926 *not* to implement a voting-by-phone system provided Constitutional questions were satisfied.

(The Colorado Constitution requires that ballots not be individually identifiable; the proposal to print telephone ballots and "voter IDs" may violate this requirement. BTW, if this information is published it can be cross-referenced with public records (of registered voters and voting patterns) in a statistical attack on the anonymity of voters. But *not* publishing this information removes one of the strongest arguments for voting-by-phone).

The ratio was quite consistent as the election results were announced, so it appeared that there was widespread distrust of this system despite substantial favorable press in the campus newspaper. Unfortunately, I don't know how much coverage the Boulder (city) paper provided; the Denver daily I read had no coverage of this issue.

Of particular interest to RISKS readers is the fact that many proponents of this measure implicitly acknowledged that a person voting out of sight of election officials could be coerced, but they felt this was "irrelevant" since people who feared being coerced could simply vote at the regular polling place! The fact that anyone who could be coerced to vote a particular way could as easily be coerced to vote by phone, instead of in person, was not recognized.

Bear Giles bear@fsl.noaa.gov

Tablespoons, or another risk?

Steve VanDevender <stevev@miser.uoregon.edu> Thu, 18 Nov 93 01:44:11 PST

The poem "Tablespoons" allegedly created by writing Lewis Carroll's "Jabberwocky" into an Apple Newton seems to have words a little too far off the originals, even given the Newton's shaky handwriting analysis, and some of

the words seem too well chosen. It really looks to me as if someone wrote a parody of "Jabberwocky" with veiled references to things from the world of computers and the Internet and passed it off with a clever framing story. It can be too easy to believe what you read on the net, especially if an author plays off of expectations well.

Charge cards from mail order houses

<wobber@src.dec.com>
Thu, 18 Nov 93 17:06:13 -0800

My wife obtained a credit card from a local branch office of a clothing retailer (Talbots) who also happens to be in the mail order business. Recently I had an opportunity to place an order using one of their catalogs that was mailed to our home.

The phone sales agent was able to look up my wife's account from a 5-digit number printed on the catalog. Now, my wife and I don't share last names. Nonetheless, the sales agent was willing to accept an order in my name, send it to a location of my choosing, and charge it to my wife's account!!

Seems like anyone who picked up the catalog from the trash could have made such an order. I'll be more wary of accepting new credit cards in the future.

Ted Wobber -- wobber@src.dec.com DEC Systems Research Center

[Worse yet, just pick five digits at random! But maybe the fact that the addresses matched made it OK. PGN]

United Parcel Service signatures

Jim Carroll <jcarroll@jacc.com> Fri, 19 Nov 1993 11:00:44 -0500

UPS (United Parcel Service) arrived at my doorstep the other day, with yet another package for delivery.

I signed the little handheld machine that they carry around, to signify my receipt of the package. I've been doing this for the last couple of years. UPS is the only courier (in Canada, in any event) to use these handy little devices.

However, I began to wonder this time about UPS and signatures. UPS must have collected my signature in digital form over 50 times now through the past few years.

Maybe my signature exists in some UPS database at this point? Maybe a smart hacker somewhere in the bowels of has figured out a way to download my signature from their field device? Maybe my digital signature can be misused in some fashion?

What are the risks that are posed by UPS collecting digital signatures? Might those risks be compounded as more companies implemented field devices such as UPS? What should we as consumers being doing to protect ourselves?

Should I even bother signing with my real signature, or should I just print out my name?

Perhaps there is an interesting issue here that RISKS should explore.

Jim Carroll, J.A. Carroll Consulting, Mississauga, Ontario jcarroll@jacc.com +1.905.855.2950 Co-Author, "The Canadian Internet Handbook", due March 1994

Re: Massachusetts state police confusion (Garfinkel, RISKS-15.26)

Brian Hawthorne,SunSelect Strategic Marketing <bri>
Suneast.east.sun.com

Mon, 22 Nov 1993 10:37:19 +0500

In <u>RISKS-15.26</u>, Simson L. Garfinkel forwarded a claim by a David Lewis of the Registry of Motor vehicles that the confusion was caused by:

"They got stickers confused with people who were supposed to get food stamps. So the people [who were supposed to get] the food stamp books got the gun permits, and the people who were supposed to get gun permits got food stamps."

I would urge Mr. Garfinkel to seek independent confirmation in the future. Were Mr. Lewis' claim to be true, it would imply that my wife was a recipient of food stamps. While she did provide graphic design services to the Department of Public Welfare for several years, she has never been a client of theirs.

Both Mr. Lewis and Eric Forak (in Risks 15.28) make the assertion that gun permits were actually ISSUED to food stamp recipients. As far as I know, the only mixup resulted a renewal application being sent to the wrong list of people. This has all the signs of degenerating into a rather nasty urban legend: "And then, the state police accidentally shipped fully automatic weapons to everyone who had ordered an MBTA pass by mail..."

Let's stop this before it escalates further. If anyone else has any verifiable information (i.e. confirmable in writing from multiple sources), let's hear it.

The current RISK? The ease of electronic communication makes small-town gossip circles look like peer-reviewed journals.

Brian Hawthorne

✓ Re: Ada Usage

Douglas W. Jones, 201H MLH, 3193350740 < jones % pyrite@uunet.uu.net >

Thu, 18 Nov 1993 15:56:48 GMT

Harry Erwin (erwin@trwacs.fp.trw.com) wrote, on 15 Nov 1993, that

> There are real problems for which Ada is not the best language.

>

- > 1. Simulation--due to the lack of support for coroutines, Simula-style
- > semaphores, condition queues, call by name, and event lists,

I have used Ada for a fairly large scale discrete event simulation project, and while I would have enjoyed having coroutines, the other issues were not problems.

Specifically, having done a fair amount of research on event lists, I simply transliterated the best I had from older Pascal code, packaged it up to hide the details behind the cloak provided by Ada's package and private type mechanisms, and used it. My event set package is in a few repositories of public domain Ada code, and I'll gladly E-mail it to anyone who wants it.

Call by name is not needed, but some form of procedure parameter would be nice. I found, though, that the lack of both never really got in the way. The generic and package mechanisms of Ada are powerful enough that I never encountered a case where they were insufficient, but they weren't always my first choice.

Coroutines would also have been nice, but their lack never stood in the way of my project. In fact, I believe that Ada's tasking features could be quite effectively used to do process oriented simulation, but I haven't investigated this (my model wasn't expressed in process oriented terms).

I was surprised to find that Ada's separation of package bodies from package definitions covers at least 90 percent of the uses I would have had for inheritance in an object oriented language. The remaining 10 percent, however, caused more than a few headaches.

The biggest thing I miss in Ada is garbage collection, but this isn't a problem with Ada, as specified, but merely a problem with all the available implementations. Why isn't garbage collection more widely available?!

Doug Jones jones@cs.uiowa.edu

✓ Re: Ada Usage

"Robert I. Eachus" <eachus@spectre.mitre.org> Thu, 18 Nov 1993 18:24:32 -0500

At a RISK of beating this horse to death, I'll respond to Harry Ervin (erwin@trwacs.fp.trw.com) who said:

> There are real problems for which Ada is not the best language.

Of course there are. Next.

- > 1. Simulation--due to the lack of support for coroutines, Simula-style
- > semaphores, condition queues, call by name, and event lists,

Have you looked at the Ada 9X standard out for ballot? Make your desires known. (Most of this list is in there, but I guarantee you won't get classical Algol 60 call by name, no matter how many comments you send in. ;-)

- > 2. Test generation--for similar reasons,
- > 3. Multi-threaded applications with external inputs, where the usual
- > tasking libraries run into problems. What happens is that the OS
- > and the run-time environment sometimes need to enter messages or events
- > into the same queues. Unless the library has been carefully integrated
- > with the operating system, race conditions can occur, losing entries.

This definitely sounds like a complaint about a bug in a particular implementation, and probably relates this to comp.risks. Do not believe that just because a compiler (or operating system) has been validated there are no bugs. On the other hand, please try not to confuse OS behavior with the properties of a programming language.

> 4. Object-oriented programming in the full sense,

Again get the Ada 9X draft and respond. Tucker Taft and a lot of others worked hard to get OOP all "in there." If there is anything missing please provide details.

> 5. Completion routines for inter-device protocols, and

For the Ada 9X Requirements Workshop several years ago in Florida, we had tee-shirts made up: "I don't know what the problem is... but Finalization is the answer." It's in there, as is support for heterogeneous distributed programming.

> 6. Anything that needs to run close to the bare metal.

It's in there. If there is something you think is missing from the Reference Manual or the Real-Time and Systems Programming annexes, please let ANSI or ISO know. (Is this starting to sound repetitious? Okay, I'll stop now.)

Robert I. Eachus

Re: UK government to scrap safety laws

Keith Lockstone <klockstone@cix.compulink.co.uk> Thu, 18 Nov 93 11:37 GMT0

This posting underlines a fundamental polarity between safety and 'free enterprise' - best summed up by:

[The Herald of] Free Enterprise puts to sea again - with its bow doors open.

Keith Lockstone



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 30

Weds 1 December 1993

Contents

Risks of automated betting

Russ Corfman

Computer Changeover May Cost \$16M

Lin Zucconi

Mercury passwords can be compromised

Keith Lockstone

Computerized Pornography

Brian Randell

Picking from Trash (Re: Charge cards from mail-order houses)

Li Gong

GRE goes "adaptive"

Cris Pedregal Martin

More news on the Lufthansa A320 accident in Warsaw

Peter B Ladkin

Memory error corrupts file

James Michael Chacon

New Moderator for the Computer Privacy Digest

Dennis G. Rears

Re: Safety-critical software

Pete Mellor

Re: Ada Usage

Tucker Taft

Mathew Lodge

Info on RISKS (comp.risks)

Risks of automated betting

Russ Corfman <corfmanr%gtephx@[130.131.0.4]> Sun, 28 Nov 93 16:58:38 MST

The following article about problems with automated gambling at a dog track was taken from the sports page of the 28 Nov 1993 Arizona Republic:

Computer Glitch costs bettor shot at \$17,000

The bettor had the right numbers and plenty of time at the window but lost a chance at \$17,000 when the computer wouldn't take his wager at the Palm Beach (Fla.) Kennel Club. "I've been betting for 35 years with horses and dogs, and this is the toughest part to take," said the man, who did not want his name used. He and his wife tried to enter six combinations, including the winning one, four minutes before post time Friday. But the computer refused to take the numbers fed by the clerk and her supervisor. They called the track trying to get the race delayed, but no one answered.

"Unfortunately, there are mistakes that are made," track spokeswoman Theresa Hume said. "We can't pay him anything unless he has the winning tickets." The man shrugged off his bad luck, saying, "I'm a gambler. I'm a bettor. That's what I do."

Russell Corfman, AG Communication Systems; Phoenix, AZ corfmanr@agcs.com UUCP: ...!{ncar!noao!enuucp | att}!gtephx!corfmanr (602) 581-4403

Computer Changeover May Cost \$16M

"Lin Zucconi" <lin_zucconi@lccmail.ocf.llnl.gov> 29 Nov 1993 15:45:15 U

Article in Saturday (Nov. 27, 1993) issues of the Valley Times says that "bugs in a new computerized hospital billing system could cost Los Angeles County up to \$16 million." The county signed a \$65M deal in 1990 for the computer system to keep track of billing and clinical treatment at county facilities. System was to be installed Jan. 1994 but that date is now Sept. 1994. The nine-month delay will cost the county \$4M to extend its countract with the company currently handling hospital billing. The system could also have up to \$2M "in extra programming and miscellaneous costs." "We thought the system was hard to work, it wasn't user friendly," said Asst. Auditor-General Mike Galindo.

Mercury passwords can be compromised

Keith Lockstone <klockstone@cix.compulink.co.uk> Wed, 24 Nov 93 13:38 GMT0

In the UK, one of the ways of accessing the Mercury phone system is to dial 131 on the British Telecom system, dial the 10 digit Mercury password and then dial the required phone number.

When making private calls from my workplace, I thought it best to use my Mercury account and pick up the cost myself.

Originally, the company exchange used pulse dialing. So, in order to make a call, I would dial 131 and then use a tome beeper to dial in the password and phone number. Thus the exchange only logged 131 as the call destination.

However, when a new company exchange was installed, the whole system went to dual standard, i.e., pulse and tone dialing. Some weeks later, I realised the

implications and asked to see the exchange log. There, of course, was my Mercury password included in the call destination field. I hastily had my Mercury password changed and have never used it this way since!

British Telecom regularly uses call loggers for traffic analysis purposes. As they do not record conversation, they do not need a warrant from the Home Secretary. The were used without a warrant in the 'Prince Philip Mailbox Hack' case (Regina v. Gold and Schifreen) to establish patterns of interconnections between individuals and on-line computer systems. Their misuse by unscrupulous BT employees could lead to a black market in Mercury passwords.

Keith Lockstone

Computerized Pornography

<Brian.Randell@newcastle.ac.uk>
Fri, 26 Nov 1993 12:07:54 GMT

The attached article is reprinted in its entirety from today's (26 Nov 1993) edition of The Independent.

The issue of pornography and portrayals of violence in computer game cartridges and disks is very high profile here at the moment - particularly this week with the ending of a much-publicised and very harrowing trial which resulted in two 11-year old boys being convicted of the brutal murder of a two-year old child, who they had enticed away from his mother in a shopping mall. In delivering the "guilty" verdict (on the youngest defendants ever to be found guilty of murder in the UK) the judge said that exposure to such material might have influenced them - the police however have disagreed. (A day or so before the trial verdict there was a lengthy documentary on TV - I didn't note the details - whose main point was that parents who in general exercise some judgement and control over the films and videos that their children watch are almost invariably unaware of, and would be horrified by, some of the material their children are exposed to via computer game cartridges and disks.)

The present government statement is not being portrayed as a response to the judge's comments, and indeed is more concerned with pornography than violence. However the atmosphere in which it has been received is for the moment at any rate very much influenced by this particular trial verdict. Brian Randell

Howard to Tackle Computerised Porn, by TERRY KIRBY, Crime Correspondent

ACTION to tackle pornographers who plan to create and trade in computer-simulated paedophile material was announced yesterday by Michael Howard, the Home Secretary.

The move is designed to plug a loophole in the law, which currently only covers indecent photographs, film and video recordings of children under the

age of 16. It will be included in the forthcoming Criminal Justice Bill, which already contains measures to toughen existing legislation covering child pornography.

There has been mounting concern among senior police officers and the Home Office following the discovery that pornographic images of women had been scanned onto computer discs, modified to appear more childlike and then had images of children's heads superimposed to create pornography of high photographic quality.

Although the equipment required costs several thousand pounds, officials are concerned that "cottage industries" could be set up to produce computer images of child pornography for the black market.

Ministers emphasised yesterday that, although only isolated examples of the trend had been identified and a case had not been brought to court, it was necessary to act swiftly because it was possible that such computer-simulated pornography could be outside existing laws, and delay could allow the pornographers to thrive.

Mr Howard said: "New technology continually presents new challenges to the law. I am determined the law should keep pace with them and I will not hesitate to act whenever those who degrade children find new means of peddling this material."

The proposals give police powers to arrest, without warrant, traffickers in child pornography and other obscene material, increase police powers of search and seizure, and improve the powers of trading standards officers.

Courts will be given powers to impose sentences of up to three months and/or a (pounds) 5,000 fine for possessing paedophile material; traders can face a maximum of three years.

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

✓ Picking from Trash (Re: Charge cards ..., Wobber, RISKS-15.29)

Li Gong <gong@csl.sri.com> Wed, 24 Nov 93 11:04:52 -0800

I've noticed that the phone companies in several states and at least one long distance carrier use (or used) the same algorithm to assign a PIN to a calling card, based solely on information about the person. Thus if you throw your old card into the trash in Massachusetts and move to California, one who picks the trash can reliably charge all his/her calls to your new California account. [I guess one can ask for a different PIN from the phone company.]

Li Gong, SRI International, Computer Science Lab, Menlo Park, California

✓ GRE goes "adaptive"

Cris Pedregal Martin <pedregal@unreal.cs.umass.edu> Mon, 15 Nov 1993 21:26:39 -0500 (EST)

Canada-US-academia readers may skip this background paragraph. The GRE is a standardized (multiple-choice, fill-in-machine-readable- form) test used by most universities as (sometimes very important) element in deciding on an applicant's admission. There's a general test, and specialized tests for a number of subjects, such as Computer Science, Math, etc.

The New York Times, 15 Nov 1993, p. A1) carries a story on using computers to give the GRE. It is written by Michael Winerip and entitled:

"No. 2 Pencil Fades As Graduate Exam Moves to Computer"

I'll sidestep the discussion on how seriously one should take standardized exams; the fact is that they make or break many an applicant. I want to focus on the way in which the computer is used. It is not just as a clever way to record the answers to a test in the usual format. The new format is "adaptive." To quote from the blurb:

... The computer randomly selects a first question of medium difficulty. If the test taker answers the question correctly, the computer poses a more difficult question. Once the test taker gives an incorrect answer, he or she is given a question at the next easiest level. Test takers are graded based on the level of difficulty they master.

This is very attractive to ETS (the company that administers these tests) for various reasons; one is that the processing of the test is trivial --as a matter of fact, it reports the result to the student as soon as she answers the last question. But more interestingly: there are many more different tests to make out of the same set of questions (they claim that in a test trial with 1200 people there were no two equal tests; the readers of RISKS are familiar with combinatorics). So there's a strong economic incentive here.

The RISKS? The usual with erroneous results coming from faulty software, and the faith most people have in computers. And more: current GRE reports scores and percentiles. The latter, but also the former, are normally taken in the context of a population. But now there will be no such thing anymore. Of course, the "testing experts" will normalize things away by assigning "values" to the questions; as any experienced teacher knows, it is quite hard to rank all questions by difficulty... as the faculty in the CS Dept used to say in the comprehensive exams here:

The number next to each question indicates its value, but budget your time carefully as we make no claim as to the relative difficulty of the questions.

There's other risks and problems; I am sure other readers will contribute to the discussion. The overall risk is to make decisions that significantly affect the functioning of the system (i.e., the choice of incoming students) based on models of reality whose validity is hard ascertain.

Cris Pedregal Martin
Computer Science Department

pedregal@cs.umass.edu
UMass / Amherst, MA 01003

More news on the Lufthansa A320 accident in Warsaw

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
1 Dec 93 21:31:32 GMT (Wed)

The story so far is that the spoilers, brakes and reverse thrust were disabled for up to 9 seconds after landing in a storm on a waterlogged runway, and the airplane ran off the end of the runway and into a conveniently placed earth bank, with resulting injuries and loss of life. (First report of actuation delay in Flight International, 13-19/10/93.) Subsequent enquiry led various people including myself to speculate that there was some sort of logic or system error, which was subsequently narrowed down to a problem with the arming logic for the spoilers-brakes-reverse-thrust combination (let's call this the braking logic for short).

On 10 Nov, Frankfurter Allgemein reported that Lufthansa had concluded there was a problem with the logic, and was requiring their pilots to land in a different configuration and a different manner in such weather and runway conditions, to 'fool' the logic. This decision was supported by the Luftfahrtbundesamt, the German equivalent of the FAA (US) or CAA (GB). Der Spiegel, in issue 47 (22/11/93) reported on the 'deadly logic' of the A320 braking systems. Der Spiegel this week (issue 48, 29/11/93) reported that Lufthansa was talking with Airbus on a change in the braking logic to reduce the weight-on-wheels load criterion from 12 metric tons to 2 metric tons, and claimed that this was the first time that Airbus had to 'convert their machines' because of an accident ('ihre Maschinen nach einem Unglueck umruesten muessen').

I talked this afternoon to David Learmount, the Operations and Safety Editor of Flight International, concerning progress on the A320 crash in Warsaw and the consequences. He holds an ATP (Airline Transport Pilot) or equivalent rating. I asked David what was afoot, since Flight International has been relatively quiet since 13/10. He said that Lufthansa, the Luftfahrtbundesamt, and Airbus are all still in conference. Firstly, the airplane is not certificated for what Lufthansa want to do. So, they are all trying to figure out what *can* be done. The certification authority (JAA, see below) may be involved in these discussions. Everyone, including David, is aware that although the solution may be implemented in software, this doesn't necessarily mean the software itself was at fault (i.e. the software may correctly implement the braking logic, but this latter may be inappropriate).

Some other information. David said that normally one carries 5-15kts for gusts. Carrying 20kts, as in Warsaw, is unusual. Secondly (confirming speculation that some pilot actions may have been contributory), the pilot tried to grease it on, rather than dumping it on. (`Dumping it on' means landing relatively hard, which is acceptable to all but the passengers, is likely to have compressed the squat switches, and also more likely to get the wheels gripping and spinning.) Thirdly, the landing was well inside the

certification envelope, which is somewhere in the region of 200kts. Additionally, there is no information to suggest that the pilot had any indication that the weather report was old. David also confirmed the 12 metric ton figure for the squat switch trigger.

The Joint Airworthiness Authority certifies (or certificates, as they say) airplanes for EU countries. Theoretically, all members of the EU are members of the JAA, but in practice only the French (DGAC), British (CAA), Germans (LBA) and Dutch (???) are active rule-makers.

Many thanks to David and Flight International for this information.

Peter Ladkin

Memory error corrupts file

James Michael Chacon <probreak@matt.ksu.ksu.edu> Sun, 28 Nov 93 05:40:18 CST

I had an interesting thing happen to me the other morning while working. According to syslog, I got a parity error somewhere in memory:

Nov 26 01:17:26 vmunix: Parity error reported at 0x8488, actual address is 0x8488.

Nov 26 01:17:26 vmunix: Parity Error, ctx = 0x2, virt addr = 0x8488

Nov 26 01:17:26 vmunix: pme = 820013b0, phys addr = 13b0488

Nov 26 01:17:26 vmunix: Parity Error Register 94<ERROR,CHECK,ERR08>

Nov 26 01:17:26 vmunix: bad module/chip at: U590

Nov 26 01:17:26 vmunix: parity error at 13b0488 is transient.

Nov 26 01:17:26 vmunix: page 13b0000 back in service.

Nov 26 01:17:26 vmunix: System operation can continue

From the looks of it, it was a transient error that fixed itself without a problem. However, right after this the load on the machine started climbing rapidly and would not come down no matter what I tried. So, I figured it was time for a reboot anyways and rebooted.

When everything came back up, I could log in ok as my shell just execs X windows on the console, but could not get a local window. Traced it down by the last modified time on my shell. Seems /usr/local/bin/bash (which is my current shell) had last been modified on Mov 26 at 1:17......

Now this is bad, I get a parity error, which corrupts a supposedly non-writable text segment page, which then gets marked as dirty so the OS flushed it back onto the disk. What's next, writing data pages back out as text pages? (This is on a Sun IPC running 4.1.3)

James

New Moderator for the Computer Privacy Digest

"Dennis G. Rears" <drears@Pica.Army.Mil> Wed, 1 Dec 93 8:28:14 EST

I will relinquish moderator duties of the Computer Privacy Digest today. Prof. L. P. Levine will take over as the new moderator of the Computer Privacy Digest (comp.society.privacy) effective midnight tonight. The new relevant addresses are:

Submissions: comp-priv@uwm.edu

Administrivia: comp-priv-request@uwm.edu

Complaints: /dev/null

The primary reason I am leaving the group is time. In the last few months I have not had the time to adequately perform the duties of being a moderator. I would like to thank all the people who have contributed to the digest and those people who have provided me with pointers on making the digest better. I have for the most part enjoyed moderating the group. I will miss the off-line discussions I have had with many of you.

The CPD had it origins in the telecom-privacy mail list which I set up in August of 1990. Telecom-priv started out to address concerns of Caller Id. It was an outgrowth of a discussion that was started on the Telecom digest. The telecom privacy maillist was merged into the Computer Privacy Digest on 27 April 1992. According to the October USENET readership report comp.society.privacy is read by about 44,000 people, 73% of USENET sites receive this and is ranked at 683. I have about 500 subscribers/exploder lists. I think we have come a long way since the first issue was published in April 1992. FTP access to the archives of the Computer Privacy Digest & the Telecom Privacy list are available at ftp.pica.army.mil and at ftp.cs.uwm.edu. I wish Professor Levine good luck in his new role. I plan to assume a role as Official Lurker.

dennis

P.S. I will remain as the keeper of the government (MIL & GOV) portion of the RISKS list. The BARFmail is still at a tolerable level.

[And once again, many thanks to Dennis for his past and future help in his nonMILitant keeping of the RISKS sublists. PGN]

★ Re: Safety-critical software (Parnas, RISKS-15.22)

Pete Mellor <pm@csr.city.ac.uk> Tue, 23 Nov 93 19:40:07 GMT

Dave Parnas <parnas@qusunt.eng.McMaster.CA> writes:-

- > Even if we did test
- > every possible path, we have not done exhaustive testing. We should
- > not ever imply that such a test would be an exhaustive test.

I totally agree, and Cliff Jones would probably agree as well. In my summary of the programme, I was trying to give a fair account of what was actually

said, without interposing my own views or comments. (Since I did not have a recording or transcript to hand when I was writing, however, the summary was dependent on my highly unreliable memory.) Cliff Jones was also constrained by broadcasting time, and the need to address a non-technical audience.

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB Tel: +44 (71) 477-8422, Fax.: +44 (71) 477-8585,

★ Re: Ada Usage (Erwin, RISKS-15.28)

Tucker Taft <stt@dsd.camb.inmet.com> Fri, 19 Nov 93 13:56:15 EST

On 15 Nov 1993, erwin@twracs.fp.trw.com (Harry Erwin) wrote:

> There are real problems for which Ada is not the best language.

I would rephrase this to say that at a given time in a given environment, one language may be more productive than another. However, this more often has to do with the experience of the development team, the availability of existing software components and tools, etc., than the inherent features of the language. It is quite possible over time to shift the balance toward a different language, through training and experience, the development of reusable software components, and the development of appropriate tools.

Below I have more detailed comments on your claims that Ada is inadequate on the basis of its inherent features. Although I don't agree with your comments, I would certainly agree that in a given software development environment, things might be set up much more productively for development in one of these areas in some other language.

However, when it comes to the DoD, they need to worry about not just the start-up costs of using a given language, but also the reliability, the quality, the maintainability, and the "transferability" of the result produced. By "transferability" I mean the ability to take the code and documentation for a system and move it to a new development (or maintenance) environment.

Transferability is a bigger concern to the DoD than most typical software developers, because the DoD generally contracts out software development, and is then generally required by law to be able to re-compete maintenance contracts on a periodic basis, unless the product is a commercial off-the-shelf product. In other words, doing the initial custom development of a DoD system is not a guarantee of life-long employment ;-).

One of the main goals of having a single (or just a few) common high-order language(s) for the DoD was to address the requirement for transferability. Of course the DoD would like to use commercial off-the-shelf products if they can solve the problem, but for some reason they haven't found many COTS submarine-based missile launch control systems (or whatever;-).

In my detailed comments below, please remember that I don't disagree with your

basic premise -- when restricted to a particular environment, any given language might not be the most productive.

However, I don't think you have a real case in the following complaints with respect to the DoD concerns. There are already DoD contractors (and others) for which Ada is already the most productive language in some or all of the areas you mention below. Of course, this is because they have made the investment in Ada training, components, and tools to reach that point. If they had made the same investment in Lisp training, Lisp components, and Lisp tools they might find Lisp is the most productive for them.

So perhaps a more fundamental question is, given two different contractors, each of which is fully trained up and ready to go in Ada or Lisp or (fill in the blank) language, which one should DoD select on a given contract. The excellent transferability of Ada, and the many inherent reliability features of Ada, makes it a good choice from the DoD perspective. And even if the two languages are similar from these perspectives, there are advantages for the DoD to stick with just one language, so that the DoD itself can build up its own expertise, components, and tools in that "common" DoD language.

- > 1. Simulation--due to the lack of support for coroutines, Simula-style
- > semaphores, condition queues, call by name, and event lists,

Ada supports "coroutines" in the sense that it supports full tasking in the language, and two tasks can hand control back and forth should they so choose. Did you have something else in mind? Semaphores, condition queues, and event lists are also easily implementable in Ada. Could you explain why call-by-name is relevant to simulation? Is it the ability to pass subprograms as parameters? This is provided in Ada 83 via generics, and in Ada 9X also via access-to-subprogram types. Generics can also be used to pass an object "by name" (formal IN OUT objects).

> 2. Test generation--for similar reasons,

Same issues.

- > 3. Multi-threaded applications with external inputs, where the usual
- > tasking libraries run into problems. ...

The "tasking library" comes with the compiler in Ada, and is required to be "carefully integrated" with the operating system if it is to conform to the definition of the language.

> 4. Object-oriented programming in the full sense,

Ada 9X supports object-oriented programming in the full sense. Ada 83 supports abstraction, modularity, information hiding, and compile-time polymorphism (generics), which are already enough to support object-oriented design.

> 5. Completion routines for inter-device protocols, and

Can you elaborate on what is a "completion routine"? Is it an event handler? This is provided via generics in Ada 83, and also via access-to-subprogram and

dispatching operations in Ada 9X. Is it an interrupt/signal handler? These are supported in both Ada 83 and Ada 9X.

> 6. Anything that needs to run close to the bare metal.

Ada 83 provides excellent support for data representation control. Ada 9X goes further.

As mentioned above, I agree with your basic premise that in a given environment, one language will be more productive than another. But I know there are software developers who are very productive in Ada in all of the areas you mention above. But of course, there are others who are more productive in some other language in these same areas (presumably do to different training, experience, components, or tools).

S. Tucker Taft Intermetrics, Inc. Cambridge, MA 02138 stt@inmet.com

✓ re: Ada Usage (Erwin, RISKS-15.28)

<lodge@ferndown.ate.slb.com> Wed, 24 Nov 93 10:39:49 GMT

While not wishing to drag RISKS into a language debate, Ada gets so much undeserved bad press that I feel I should comment on Harry's assertions:

- > 3. Multi-threaded applications with external inputs, where the usual
- > tasking libraries run into problems. ...

This isn't a problem with Ada per-se -- just one particular implementation. Ada run time systems today are very well integrated with the OS on UNIX platforms, for example. There are several Ada RTSes that implement tasking on top of POSIX threads for excellent task and I/O handling.

You get even better implementation on "bare targets" with no OS, since the RTS doesn't have to work around the OS to get the real time performance some users require.

> 4. Object-oriented programming in the full sense,

True, there's no inheritance or polymorphism, but then both of these are largely incompatible with real-time software (one of Ada's target application areas). Dispatching routines for objects introduce variable run-time overheads that most real time people would rather do without.

Having said that, Ada 9X *does* provide full OO programming (get the latest pre-release version of GNU-Ada 9x from ftp.nyu.edu if you're interested).

> 6. Anything that needs to run close to the bare metal.

I've written Ada that runs very efficiently on "bare metal" Transputer networks. I think that qualifies as a counter example to the blanket "everything".

Ada is certainly no panacea for RISKy programming problems. Then again, a colleague has just spent the last six hours tracking down a bug in a C program that turned out to be caused by an array index out of range -- something that an Ada program would have pointed out immediately.

Mathew Lodge Schlumberger Technologies, ATE division, Ferndown, UK lodge@ferndown.ate.slb.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 31

Friday 3 December 1993

Contents

London Underground train departs driverless with 150 passengers

Voting by Fax

Bear Giles

Computer Fax Problems

Martyn Thomas

Andrew Blyth

A study of National Cryptography Policy

Mariory Blumenthal

- "Using McAfee Associates Software for Safe Computing" by Jacobson **Rob Slade**
- New Docs Reveal NSA Role in Digital Telephony Proposal **Dave Banisar**

Re: Computerized Pornography

Charlie Stross

Re: Lufthansa Airbus Warsaw Crash 14 Sep 93

Udo Voges

Re: Mercury passwords can be compromised Peter Debenham

Re: United Parcel Service signatures

Andrew Marc Greene

CFP: 13th Symp. on Reliable Distributed Systems

Rick Schlichting

Info on RISKS (comp.risks)

London Underground train departs driverless with 150 passengers

Martyn Thomas <mct@praxis.co.uk> Thu, 2 Dec 1993 17:29:24 +0000 (GMT)

According to BBC Radio 4 news (17.00 Dec 2nd), a Picadilly Line underground train travelled 1.5 miles at 20-40 mph including going through Caledonian Road station, without a driver.

The driver (and sole crew) had got out to close a door "without carrying out

the proper procedure to shut down the drive systems" according to a spokesman for London transport.

The train stopped automatically at a red light, and was boarded by LT staff who had commandeered the following train and given chase.

No passenger pressed the emergency alarm - but it wouldn't have helped as it just rings a bell in the driver's cab.

A colleague believes that there is a "dead-man's handle" which the driver must have disabled. My theory is that the train had decided to play Mornington Crescent and seized its opportunity. --

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

[I presume this is a NEW incident. RISKS-9.81 described a case contributed by Stephen Page: On 10 Apr 1990, the driver of an Underground train had taped down the drive control, relying instead on the doors being closed to enable the train to move forward. He then left the train to see why the doors had not closed. The doors closed, and the train took off. But Martyn's report sounds like the same story! Maybe it was just the same driver, 3.6 years later. PGN]

★ Re: Mercury passwords can be compromised (Lockstone, RISKS-15.30)

<PMDebenham@email.meto.govt.uk> Thu, 02 Dec 1993 16:29:40 +0000 (GMT)

Keith Lockstone noted the problem of call loggers catching his Mercury Telephone system password when using the system from work to access his personal Mercury account.

The phone directory of numerous places where I have worked have in their user information the fact that using British Telecom charge cards should not be done because of call loggers picking up the card password. The same applies to Mercury passwords clearly.

The risk? The standard one of sending passwords in the open through a system which is not secure. Namely the fact that it is not possible to ensure the password is not intercepted. Think of all the passwords being passed in clear form over tcp/ip links - then shudder!

For Mercury, at least the phone number and time of every call is on the bill allowing you to check usage. Of course for Mercury you could also use the non-passworded (132) system where Mercury picks up the number you are calling from as the basis for charging. There though you cannot do useful things like cost centres (yet!)

Peter Debenham, Rm165, APR, Meteorological Office, London Rd., Bracknell, Berks., UK. RG12 2SZ tel: +44 (0)344 856974(wk)

Voting by Fax

Bear Giles <bear@fsl.noaa.gov> Tue, 30 Nov 93 14:02:16 -0700

The 30 Nov 1993 edition of the _Rocky Mountain News_ (Denver) reports that Wyoming Secretary of State Kathy Karpan is considering legislation to allow overseas Wyoming residents *fax* in their ballots, to "improve" the absentee-voting process.

Bear Giles bear@fsl.noaa.gov/cs.colorado.edu

Computer Fax Problems

Andrew Blyth <A.J.C.Blyth@newcastle.ac.uk>
Thu, 2 Dec 93 10:14:27 GMT

The following is taken from the BBC television programme called WatchDog. This programme is screened on a Monday evenings at 7:30pm (GMT - UK).

I am recounting this story as best I can - however I am only human.

Today (29th Nov 93) they described a man which had been driven to take pills to calm him down by an anonymous phone caller. This caller would ring him up in the middle of the night and wake him up. He contacted BT (British Telecom) and they tried to trace the call for him. However due various factors they could only tell him the area from which the phone call was originating. He did get to the phone one night and discovered that his caller was not human but a machine. So BT lent him a FAX machine with which to receive the call.

From the faxed message it was possible to work out from where the fax communication originated. BT went to the company concerned and told them what was happening. It turned out that one of their FAX machines had been trying to send this one fax over and over again.

All this took about two years and in the process the gentleman described was driven to pills - and all the company would say to him at the end of the day was sorry.

Moral: don't put your phone number of your FAX transmissions.

Andrew Blyth, Department of Computer Science, 20 Windsor Terrace, University of Newcastle Upon Tyne, Newcastle Upon Tyne, England NE1 7RU

A study of National Cryptography Policy

"Marjory Blumenthal" <mblument@nas.edu> Thu, 02 Dec 93 08:45:28 EST

As part of the Defense Authorization Bill for FY 1994, the U.S. Congress has

asked the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) to undertake a study of national policy with respect to the use and regulation of cryptography. The report of the study committee is due two years after all necessary security clearances have been processed, probably sometime summer 1996, and is subject to NRC review procedures. The legislation states that 120 days after the day on which the report is submitted to the Secretary of Defense, the Secretary shall submit the report to the Committees on Armed Services, Intelligence, Commerce, and the Judiciary of the Senate and House of Representatives in unclassified form, with classified annexes as necessary.

This study is expected to address the appropriate balance in cryptography policy among various national interests (e.g., U.S. economic competitiveness (especially with respect to export controls), national security, law enforcement, and the protection of the privacy rights of individuals), and the strength of various cryptographic technologies known today and anticipated in the future that are relevant for commercial purposes. The federal process through which national cryptography policy has been formulated is also expected to be a topic of consideration, and, if appropriate, the project will address recommendations for improving the formulation of national cryptographic policy in the future.

This project, like other NRC projects, will depend heavily on input from industry, academia, and other communities in the concerned public. Apart from the study committee (described below), briefings and consultations from interested parties will be arranged and others will be involved as anonymous peer reviewers.

It is expected that the study committee will be a high-level group that will command credibility and respect across the range of government, academic, commercial, and private interests. The committee will include members with expertise in areas such as:

- relevant computer and communications technology;
- cryptographic technologies and cryptanalysis;
- foreign, national security, and intelligence affairs;
- law enforcement;
- commercial interests; and
- privacy and consumer interests.

All committee members (and associated staff) will have to be cleared at the "SI/TK" level; provisions have been made to expedite the processing of security clearances for those who do not currently have them. Committee members will be chosen for their stature, expertise, and seniority in their fields; their willingness to listen and consider fairly other points of view; and their ability to contribute to the formulation of consensus positions. The committee as a whole will be chosen to reflect the range of judgment and opinion on the subject under consideration.

The detailed composition of the committee has not yet been decided; suggestions for committee members are sought from the community at large. Note that NRC rules regarding conflict of interest forbid the selection as committee members of individuals that have substantial personal financial interests that might be significantly affected by the outcome of the study.

Please forward suggestions for people to participate in this project to CSTB@NAS.EDU by DECEMBER 17, 1993; please include their institutional affiliations, their field(s) of expertise, a note describing how the criteria described above apply to them, and a way to contact them. For our administrative convenience, please put in the "SUBJECT:" field of your message the words "crypto person".

Finally, some people have expressed concern about the fact that the project will involve consideration of classified material. Arguments can and have been made on both sides of this point, but in any event this particular ground rule was established by the U.S. Congress, not by the CSTB. Whether one agrees or disagrees with the asserted need for classification, the task at hand is to do the best possible job given this constraint.

On the National Research Council

The National Research Council (NRC) is the operating arm of the Academy complex, which includes the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The NRC is a source of impartial and independent advice to the federal government and other policy makers that is able to bring to bear the best scientific and technical talent in the nation to answer questions of national significance. In addition, it often acts as a neutral party in convening meetings among multiple stakeholders on any given issue, thereby facilitating the generation of consensus on controversial issues.

The Computer Science and Telecommunications Board (CSTB) of the NRC considers technical and policy issues pertaining to computer science, telecommunications, and associated technologies. CSTB monitors the health of the computer science, computing technology, and telecommunications fields, including attention as appropriate to the issues of human resources and information infrastructure and initiates studies involving computer science, computing technology, and telecommunications as critical resources and sources of national economic strength. A list of CSTB publications is available on request.

"Using McAfee Associates Software for Safe Computing" by Jacobson

"Rob Slade, Ed. DECrypt & ComNet, VARUG rep." <roberts@decus.arc.ab.ca> 26 Nov 93 9:58 -0600

BKUMASSC.RVW 930817

International Security Technology Inc.

99 Park Avenue, 11th Floor, New York, NY 10016
212-557-0900 fax: 212-808-5206

"Using McAfee Associates Software for Safe Computing", Jacobsen, 1990

There are many books which are aimed at helping you use specific commercial programs. Usually, however, such books are either targeted at "dummies" or purpose to reveal secret or undocumented features. The title here seems to suggest both a generic goal, safe computing, and a specific means. Those "in

the know" of course, realize that safety here is being limited to protection against viral programs.

Certain other works have been associated with the company named here, and have resulted in rather unfortunate products. In the Foreword and Preface we see the game "rah, rah" chauvinism. It is, therefore, a rather pleasant surprise to find that chapter one, in defining viral programs, doesn't do a bad job. A computer virus is said to execute with other programs, but that explanation is immediately extended with a lucid and factual account of the boot sequence on MS-DOS computers. It even distinguishes between the boot sector and the master boot record (although Jacobson loses points for referring to the MBR as the partition table.)

The rigorous will find errors in the first chapter. Program infection is shown strictly in terms of an appending virus. Although FAT or system viri (referred to as "cluster-point") are described, companion viri are not. The statement is made that "viruses may include a Trojan Horse": the definition is that of a trojan, the examples are clearly logic bombs.

Chapter two is entitled "Planning a Virus Control Program". This would seem to be concerned with establishing the level of risk for a company and producing policy and procedures for virus protection. Unfortunately, the detail included here is very sparse. Some extremely broad guidelines are given, but the reader is literally left with more questions than answers after reading this chapter. Eventually a companion volume by the same author is mentioned as dealing with the details.

At the beginning of chapter two one is told that chapter three, "Virus Prevention Techniques" gives the answers for protecting a single computer. Rule one: write protect everything. Rule two: Buy SCAN. Rule three: buy *more* SCAN. Rule four: have extra copies of SCAN around (be sure to buy extra licences.)

Chapters four to seven are basically reworkings of the documentation for VSHIELD, SCAN, CLEAN and the network uses thereof. One immediately asks, of course, which version was used. One is not immediately answered: chapter eight indicates, and nine supports, the presumption that version 85 was used. In the mailing with my review copy I received a letter indicating that update files are produced. The files, USINGxxx.ZIP, where xxx is the version number, are stated to be available on the McAfee BBS and the McAfee forum on Compuserve. Apparently the updating is not constant: the "current" version of the McAfee products, as this was received, was 106, and had been for some time. According to the letter, the "current" version was USING102 and USING106 was due out shortly.

Chapters eight and nine tell you how to get technical support, first, and a copy of the program, second. The answers are to call the McAfee BBS, the McAfee Compuserve forum, or call McAfee Associates and buy it. An order form for the McAfee products is bound into the back of the book: it will surprise no one that the publisher of the book is a McAfee agent.

Chapter ten is entitled "The Ten Most Common Viruses". Those familiar with the sometimes unfortunate accuracy of the VSUM lists will recognize the entries. In a listing at the end of the chapter, BRAIN and Stoned are included in a list of "stealth" viri which can cause "catastrophic damage" or "cause all files to become infected during the scanning process".

Essentially, what you have here is printed (and dated) documentation for the McAfee programs. Since the functions of the programs change less frequently than the scan strings, most of the material is still relevant. Problems can be checked against the current McAfee documentation. As such, this may be a useful book, fairly reasonably priced considering the cost of the programs themselves. One shortcoming is that the network section still relies on the combination of stand-alone software: the NLM versions are not mentioned. In contrast to most "third party" books, though, there is little here that will either change the performance or ease the use, of the product under discussion.

DECUS Canada Communications, Desktop, Education and Security group newsletters Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733 DECUS Symposium '94, Vancouver, BC, Mar 1-3, 1994, contact: rulag@decus.ca

✓ New Docs Reveal NSA Role in Digital Telephony Proposal

Dave Banisar <banisar@washofc.cpsr.org>
Wed, 1 Dec 1993 14:54:51 EST

>From the CPSR Alert 2.06 (Dec. 1, 1993)

A series of memoranda received by CPSR from the Department of Commerce last week indicate that the National Security Agency was actively involved in the 1992 FBI Digital Telephony Proposal. Two weeks ago, documents received by CPSR indicated that the FBI proposal, code named "Operation Root Canal," was pushed forward even after reports from the field found no cases where electronic surveillance was hampered by new technologies. The documents also revealed that the Digital Signature Standard was viewed by the FBI as "[t]he first step in our plan to deal with the encryption issue."

The earliest memo is dated July 5, 1991, just a few weeks after the Senate withdrew a Sense of Congress provision from S-266, the Omnibus Crime Bill of 1991, that encouraged service and equipment providers to ensure that their equipment would "permit the government to obtain the plain text contents of voice, data and other communications...." The documents consist of a series of fax transmittal sheets and memos from the Office of Legal Counsel in the Department of Commerce to the National Security Agency. Many attachments and drafts, including more detailed descriptions of the NSA's proposals, were withheld or released with substantial deletions.

Also included in the documents is a previously released public statement by the National Telecommunications and Information Administration entitled "Technological Competitiveness and Policy Concerns." The document was requested by Rep. Jack Brooks and states that the proposal

could obstruct or distort telecommunications technology development by limiting fiber optic transmission, ISDN, digital cellular services and other technologies until they are modified, ... could impair the security of business communications ... that could facilitate not only lawful government interception, but unlawful interception by others, [and] could impose industries ability to offer new services and technologies.

CPSR is planning to appeal the Commerce Department's decision to withhold many of the documents.

To subscribe to the Alert, send the message:

"subscribe cpsr

★ Re: Computerized Pornography (Randell, RISKS-15.30)

Charlie Stross <charless@sco.com> Thu, 2 Dec 1993 10:39:14 +0000 (GMT)

The obvious RISK of this proposed law is that the evidence in question -- on-line pornographic material -- is fungible. It would be fairly easy for a police officer with a copy of PhotoShop to modify legal or quasi-legal images stored on a confiscated personal computer by adding, for example, a child's head to the image -- and thus "fit up" a victim for a jail sentence as a child pornographer. Such tampering would be very difficult to prove.

In case this sounds paranoid, several police officers in the UK have in the past couple of years, been found to have tampered with evidence in a number of cases. The classic instance was the West Midlands Serious Crime Squad, which was disbanded under intense public scrutiny. It was found that officers had consistently perverted the course of justice, and forged confessions and evidence against people who were imprisoned as a consequence of this.

Charlie Stross is charless@sco.com, charlie@antipope.demon.co.uk

Re: Lufthansa Airbus Warsaw Crash 14 Sep 93

Udo Voges <voges@iai.kfk.de> Wed, 1 Dec 93 09:26:48 +0100

According to TV-news and dpa, the A320 crash had three causes:

- 1. bad weather (heavy rain, wind from rear) on new runway without rain gutter
- 2. wrong weather report from the tower (light rain and wind from ahead/side)
- 3. control system enables thrust reverse etc only if both wheels carry at least 12 t weight.

Due to 1+2, touch down was some 900 m late and only with one wheel on slippery runway. Due to 3 (+above) no braking power by thrust reverse for some 8-10 sec., it was not possible to override the control system.

Airbus finally agreed to modify its control system to enable landing/braking actions already if the weight on the wheels is 2t. (Is this restriction due to e.g., the Lauda Air crash of a Boeing with thrust reverse enabled during flight?) Airbus is not willing to allow overruling of this control system.

Udo Voges, Kernforschungszentrum Karlsruhe GmbH, Institut fuer Angewandte Informatik, Postfach 3640, D-76021 Karlsruhe, GERMANY +49-7247-82-5725

[This echoes what Peter Ladkin contributed to <u>RISKS-15.30</u>, and is included for those of you who did not go through Peter's account. PGN]

★ Re: United Parcel Service signatures (Carroll, RISKS-15.29)

<Andrew_Marc_Greene@frankston.com>
Wed, 24 Nov 1993 10:22 -0400

As the president of my company pointed out when I asked him why he kept the bitmap of his signature in a directory readable by anyone in the company, "Anyone who has my signature, a fax machine, and a fax modem can sign whatever he wants with my name anyway." (That's how he got the bitmap in the first place.)

- Andrew Greene

✓ CFP: 13th Symp. on Reliable Distributed Systems

Rick Schlichting <rick@cs.arizona.edu>
30 Nov 1993 22:38:29 -0700

CALL FOR PAPERS

13th Symposium on
Reliable Distributed Systems
Oct. 25 (Tues), 1994 - Oct. 27 (Thurs), 1994
Dana Point, California

SPONSORS:

IEEE Computer Society TC on Distributed Processing
IEEE Computer Society TC on Fault-Tolerant Computing
IFIP WG 10.4 on Dependable Computing

THEME:

The theme of the symposium is reliability of distributed and parallel systems, including distributed applications, distributed operating systems, and distributed databases. Papers are sought that address the reliability, availability, security, and performance aspects of distributed and parallel systems. Papers that deal with experimental results, testbeds, development, and data from operational systems are of particular interest.

TOPICS OF INTEREST:

The following topics, as they relate to distributed and parallel systems, are of interest to the Symposium:

- System-Level and Software Fault Tolerance
- Fault-Tolerance Formalism
- Database Systems
- Operating Systems
- Security
- Experimental Systems with High Reliability Mechanisms
- Object-Oriented Systems
- Transaction Processing Systems
- Performance and Reliability Modeling
- Programming Language Support for Reliable Computing
- Real-Time Fault-Tolerance

PAPER SUBMISSIONS:

Papers must be written in English and printed using at least 11-point type and 1-1/2 line spacing. They should be no more than 20 pages in manuscript, including figures. Authors are requested to submit five copies of their manuscript by March 15, 1994 to:

Prof. Richard D. Schlichting
Department of Computer Science
Gould-Simpson Building
The University of Arizona
Tucson, AZ 85721, USA

+1-602-621-4324 rick@cs.arizona.edu

Authors will be notified by June 1, 1994. Final camera-ready copies are due July 9, 1994.

AWARDS:

The Wing Toy Best Student Paper Award, carrying a monetary award, will be given to the best student paper accepted for the Symposium. A paper is eligible for the award only if (1) it will be presented at the Symposium by a student co-author, and (2) the research it presents is essentially the work of the student co-authors and the involvement of the non-student co-authors was restricted to advising the student co-authors. The detailed Award rules will be provided to the authors of the accepted papers.

TUTORIALS:

Persons interested in teaching a half-day or full-day tutorial on topics related to the theme of the symposium are encouraged to submit a proposal with a brief syllabus by March 15, 1994 to:

Dr. Devesh Bhatt Honeywell Systems & Research Center 3660 Technology Drive MN65-2100 Minneapolis, MN 55418, USA

+1-612-951-7316 bhatt@src.honeywell.com

SYMPOSIUM CO-CHAIRS:

Kane Kim

University of California, Irvine

Algirdas Avizienis

University of California, Los Angeles



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 32

Tuesday 7 December 1993

Contents

FAX sends instead of receives

John McKay

Risks of conference calls "lack of announcement"

PGN

Apple Computer Distributes a CD-ROM with a "Trojan Horse"

Saul Tannenbaum

French Wiretaps

Mich Kabay

Tokyo bank fraud

Mich Kabay

German Radicals use Computers

Mich Kabay

NJ credit thefts

Mich Kabay

Counterfeits

Mich Kabay

AIDS data stolen in Florida

Mich Kabay

Unauthorized changes of address

George Zmijewski

Massive credit card fraud

Mich Kabay

Lufthansa Warsaw crash - A Clarification

Peter B Ladkin

Reminder for DCCA-4: Fourth IFIP Working Conference

Flaviu Cristian

Info on RISKS (comp.risks)

FAX sends instead of receives

John McKay <mckay@alcor.concordia.ca> Tue, 7 Dec 1993 16:56:43 -0500

Today I tried to send a FAX to a local lawyer. It dialed but instead of

reading the paper it generated a copy of a document from the lawyer to a Canadian Embassy many thousands of miles away. Moral: Don't use FAX if you want it to get there!

[A fine example of a nonatomic transaction at the lawyer's end. PGN]

Risks of conference calls "lack of announcement"

<remail@tamsun.tamu.edu>
Tue, 7 Dec 93 10:55:38 -0600

Comments: This message DID NOT originate from the address listed in the From line. It was remailed by an automated remailing service operating at that address. Please report problems by mailing to <remail@tamsun.tamu.edu> with the subject header of PROBLEM.

Recently I had a coworker at our HQ arrange to "pull me in" to a conference call a vendor had arranged. We had a conversation about their product, after which I hung up. After I left, apparently the vendor techs all discussed the number of bugs in their product, and how glad they were that I would not be able to evaluate it for several weeks, since that gave them time to fix them.

How did I know this? My coworker noticed them still on the line, and after turning "mute" on with his phone, rejoined the conversation.

The risks are obvious. This was a computer security vendor no less!

Apple Computer Distributes a CD-ROM with a "Trojan Horse"

Saul Tannenbaum <saul@hnrc.tufts.edu> Sun, 05 Dec 1993 20:54:58 -0500 (EST)

Apple Software Dispatch is Apple Computer's new way to buy application software. They send you a CD (mine came unsolicited in the mail, but there are ads for it in MacWeek, etc.). You run an application on the CD, register your CD by a code that comes with the package, and then you can call an 800 number to purchase applications on the CD. You give them a credit card number - they give you some code number that unlocks/decrypts the application.

While the documentation nowhere says so, the registration process installs a System Extension onto your startup disk.

[Technical digression - System Extensions (sometimes called INITs), are pieces of code that execute at system initialization time that add to or modify the function of Apple System Software. They do this by intercepting calls to system routines and executing before, in place of, or after the builtin routine. This is considered a normal practice, and is used by Apple and 3rd parties extensively. A serious Macintosh configuration issue is the possibility that some set of extension conflict in some way. For example, if they intercept the same system routine, they may make the assumption

that they are the only piece of code to do so. Debugging this can be time consuming - the last extension you add may uncover problems with an extension that to that time has been trusted and stable. Thus, careful Mac users are _very_ conservative about adding extensions and do things like configure anti-viral software to warn of new extensions being added.]

The documentation left me with the impression that some sort of data file with decryption keys or, perhaps, licensing information, would be left on my system, though, again, there is nothing that says that. The only warning I had was from anti-viral software, telling me that a new extension was being put in place when I ran the registration program.

Unfortunately, on my system, this extension clearly conflicted with something, rendering my disks (hard, floppy _and_ CD-ROM) unmountable. Removing the extension fixed the problem. Booting with Software Dispatch as the only extension also worked, so Software Dispatch is not inherently buggy - it just suffers from classic Mac extension conflict problems. However, since this extension is not mentioned in the documentation, there are people who are in for a rude shock. And, since the symptoms for this problem are just a dialog saying "This disk is unreadable on this Macintosh. Would you like to initialize it?", there are people who are going to waste endless amounts of time, restoring and rebuilding their disks needlessly. After they do that, if they still don't notice the Software Dispatch extension, they still won't have fixed the problem. And, if they reinstall Software Dispatch, they'll see the problem again.

I can't believe that I'm the only person to whom this has happened. While I run a fairly complex Mac, I am relatively conservative about system extensions - with one or two exceptions, the extensions I have aren't particularly funky, they're from Apple or 3rd party vendors. I expect that Apple will be suffering from real grief about this, and, regrettably, they deserve every little bit of it.

I should note that I did report this to Software Dispatch tech support. They took all the information and promised to get back to me. I'm still waiting.

Saul Tannenbaum, Manager, Scientific Computing, USDA Human Nutrition Research Center on Aging at Tufts University Internet: SAUL@HNRC.TUFTS.EDU

French Wiretaps

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
05 Dec 93 11:17:57 EST

>From Reuter newswire via Executive News Service (GO ENS) on CompuServe, 2 Dec 1993:

Mitterrand Guard Says Elysee Ordered Phone Bugging

PARIS, Dec 2 (Reuter) - A former senior security guard of French President Francois Mitterrand told a magistrate on Thursday the president's office had ordered illegal buggings of journalists and politicians a decade ago, his

lawyer said.

The article continues with details of the taps. Main points:

- o organized by the deputy director of the cabinet;
- "computerised file" set up to process buggings in many parts of the government and also in the offices of lawyers, journalists, actors, politicians, and writers.
- o A probe is now under way.

[Just what did the "computerised file" involve? Anyone with details, please contribute.]

Michel E. Kabay, Ph.D. / Director of Education / Natl Computer Security Assoc

Tokyo bank fraud

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
05 Dec 93 11:18:22 EST

>From United Press International newswire via Executive News Service (GO ENS) on Compuserve, 3 Dec 1993:

TOKYO (UPI) -- Police arrested a former bank official and two advertising agency executives Friday on suspicion of fraud for allegedly stealing nearly \$550,000 using a computer.

The article goes on to explain that the accused, Masuji Yamashita (a bank official), and Yasuo Ueno and Yoichiro Suzuki (clients) are alleged to have made 15 fraudulent computer entries transferring the equivalent of U\$497,000 from Sakura Bank to the account of an advertising agency, Ken Enterprises. The fraud occurred over about a month (1 Feb to 4 Mar 93). "Yamashita reportedly moved the money from Ken's checking account to its savings account as cash deposits. Ken Enterprises used the funds to service its payable drafts."

[Seems like over-commitment to client service.]

Michel E. Kabay, Ph.D. / Director of Education / Natl Computer Security Assoc.

German Radicals use Computers

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 07 Dec 93 10:49:36 EST

>From United Press International newswire via Executive News Service (GO ENS) on Compuserve, 6 Dec 1993:

German radicals spy on ideological rivals

BONN (UPI) -- German rightist and leftist radicals are spying on each other and drawing up hit lists of their respective enemies, the Spiegel newsweekly said in its latest issue.

The issue that went on sale Monday sketched a frightening picture of increasingly well organized violent radicals using computer networks and undercover operations to gather and distribute information on those they consider their enemies."

The article also mentions computer-based training in how to make bombs.

[This development is important because it will bring criminal use of computers and networks to public and political attention. Unless knowledgeable people increase the pace of public education and awareness about computers and security, there will be hasty and ill-advised measures to restrict computer/network usage. Watch Germany closely in the next year or two to see the future elsewhere.

Comments from the ground in Germany, anyone? MK]

Michel E. Kabay, Ph.D. / Director of Education / Natl Computer Security Assoc.

✓ NJ credit thefts

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 07 Dec 93 10:50:07 EST

>From Associated Press newswire via Executive News Service (GO ENS) on Compuserve, 7 Dec 1993:

NEWARK, N.J. (AP) -- Fifteen salespeople at a car dealership were charged with using the credit records of more than 450 people to steal millions of dollars.

The salespeople tapped into credit reports through their computers, used the information to change the victims' addresses, and then ordered credit cards and ran up charges, Secret Service agent Peter A. Cavicchia said.

They also allegedly used the credit information to obtain bank loans and cash advances."

The article goes on to say that the average theft was \$7,500. Although the victims don't have to pay that amount, they do have to waste their time trying to correct their credit records. Apparently Autoland managers noticed the excessive and unauthorized use of their computers and reported their suspicions to the police.

Michel E. Kabay, Ph.D. / Director of Education / Natl Computer Security Assoc.

Counterfeits

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 05 Dec 93 15:50:23 EST >From Reuter newswire via Executive News Service (GO ENS) on Compuserve, 4 Dec 1993:

Customs Declare Counterfeiting Is Here to Stay (By Steven Heilbronner) FLORENCE, Italy, Dec 5 (Reuter) - British customs officials were puzzled to discover that the source of counterfeit Estee Lauder perfume was war-ravaged Bosnia. Puzzled, but not surprised, because in spite of recent seizures of counterfeit goods in Italy, Britain, Germany and France, European customs agents acknowledge they are fighting a war on so many fronts that they cannot win it."

The article discusses many non-computer counterfeits, but my eye was caught by the following points:

- o "At Nintendo, the Japanese manufacturer of video games, executives estimate losses caused by piracy at \$10 million a year."
- o Companies are hiring security specialists to tackle the problem.

Michel E. Kabay, Ph.D. / Director of Education / Natl Computer Security Assoc.

AIDS data stolen in Florida

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 05 Dec 93 15:50:41 EST

[The Associated Press reported on 4 Dec 1993 that the computerized records of at least 6000 people with AIDS or HIV were stolen from the Jackson Memorial Hospital in Miami. Three PCs and several diskettes were stolen. PGN abstracting]

The article goes on with details:

- o Crime discovered 15 Nov but not made public "for fear of alarming patients."
- o Florida Department of Health and Rehabilitative Services currently reviewing security at county facilities and AIDS clinics.

The risk to the patients is extortion. In today's highly-charged atmosphere, being identified as HIV-positive has about the same social effect as a bubo during the Black Plague (even though in fact AIDS is not very communicable in non-intimate social contacts). I hope anyone victimized goes to the police immediately if they are threatened with disclosure of their status.

Michel E. Kabay, Ph.D. / Director of Education / Natl Computer Security Assoc.

Unauthorized changes of address (Re: Kuenning, RISKS-15.11)

George Zmijewski <mzmijews@mgzcs.demon.co.uk> Sun, 5 Dec 93 0:11:21 GMT In UK when you move the house you ask Royal Mail to forward all letters addressed to you to your new address. You can apply for this service by post or in person. A day or two after receiving your application for redirection Royal Mail sends letter informing you that such service has been requested; this letter is clearly marked DO NOT REDIRECT, DELIVER TO ORYGINAL ADDRESS. This system was in practice 5 years ago when I used it for the first time. It is the only company which seems to understand that change of address can be requested by fraudsters. -- George Zmijewski mzmijews@mgzcs.demon.co.uk

Massive credit card fraud

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 05 Dec 93 11:15:04 EST

>From the Washington Post newswire via Executive News Service (GO ENS) on CompuServe, 2 Dec 1993:

Credit Scam Targets Mailboxes; 9 Postal Workers Among 40 Arrested in Washington Area Thefts (Serge F. Kovaleski / Washington Post Staff Writer)

Thousands of Washington area residents have been targeted by sophisticated scam artists who have pilfered mail from homes and post offices to get credit cards, checkbooks and information that they have used to steal millions of dollars, authorities said.

The article continues with details of the fraud, none of which will surprise readers of RISKS. Salient features:

- Thieves monitor external mailboxes on homes for weeks in wealthy neighbourhoods to steal credit cards and new cheques arriving in the mail.
- Pre-approved applications for credit cards are particularly vulnerable, since the thieves fill them out, send them in, and then intercept them shortly after postal delivery.
- The thieves impersonate bank officials to obtain personal information from victims, then impersonate the victims when they call banks for new personal identification numbers.
- o Some victims have seen as much as \$300,000 stolen through their accounts; the credit card companies (which is to say, all users of the cards) have swallowed the charges.
- A task force has been formed including members of "the Postal Service, the Immigration an Naturalization Service, the Drug Enforcement Administration, D.C. police and other local law enforcement agencies."
- Theft has struck hundreds of people in some neighbourhoods, and residents are organizing to repair insecure mailboxes and watch over them.

- o Some residents are renting Post Office boxes.
- Current credit-card and bank fraud cost about \$4 billion a year in the U.S.

Banks and credit-card providers have been reluctant to discuss security measures [trusting to the discredited principle of security by obscurity--MK]. Nonetheless, the authors note, certain changes are already being implemented:

- o Some new credit cards don't work until the card owner confirms receipt [This alone will not stop the thieves, but see next point.--MK]
- o To authenticate the card holder before activating the card, officials will use a personal profile, asking for previously-registered details of personal life. [This won't stop the criminals who fill out new card applications and give false information.--MK]
- The credit thieves use classical scavenging techniques: stealing all mail to learn about a victim, or dumpster diving to retrieve discarded documents with tidbits of personal information.
- o Some thieves have re-recorded fraudulent information on discarded, expired cards and used them successfully.

Additional comments by MK:

At first glance, one might ask how such crimes are relevant for RISKS readers. I think we should be watching these developments because credit cards have become the most widely-used access-control tokens on the planet. Because their use is usually mediated by other people, it may not seem obvious to naive users that they are in fact using computer networks for electronic data interchange. It is when credit and debit cards are personally inserted into an automatic teller machine that the close link to computer networks should be evident to everyone.

As access-control tokens, most credit cards are weaker than debit cards. At least debit cards require manual input of a personal identification number (PIN) at all times. Why don't credit card companies require a PIN too?

In Canada, some banks send credit cards only by registered mail. This sounds good in theory, but in fact I have never been asked for identification. I have often sent a clerk to collect registered mail and parcels without any trouble at all. Holding the notification card seems to be all that is demanded by clerks at Canada Post. We must sign a register, but such signatures cannot be verified and are thus useless. Perhaps banks will be interested in requesting improved authentication measures by postal employees.

In the U.S., some credit cards include a digitized photograph laminated into the card. This technique presumably reduces fraudulent use in person, but does not yet affect use in banking machines or by phone. Photos would not stop fraud by thieves who steal application forms and create new cards, but it would help when legitimate cards are stolen.

Use of cards over the phone must be the easiest channel for abuse. Because

there is no PIN, there is no authentication at all. Simply reciting a number suffices to debit the credit-card account as long as the card is currently valid. If a PIN _were_ required, how could it be recorded by the sales person without compromising the card's security? I think there should be a method for entering card numbers and PINs via touch-tone phone panel; such a system should preclude the order-taker from seeing the account number or at least the PIN. If a direct link between the customer's phone and the validation system were not feasible or affordable, an encryption routine on the receiving end could convert the transmitted PIN into a temporary, time/date-dependent version which would be unusable at any other time. This cryptogram would then be manually entered into the validation system by the order-taker.

Decisions on improving security boil down to cost and benefit, as always. As long as interest rates and card services charges are still acceptable to the victims, er, users of these services, there will be little incentive to change. I look forward to seeing a credit card company with the vision to protect its users and succeed in lowering costs as a result of lowered fraud. Then the industry will change its ways.

Michel E. Kabay, Ph.D. / Dir. of Education / Natl Computer Security Assoc.

Lufthansa Warsaw crash - A Clarification [Voges, RISKS-15.31]

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 4 Dec 93 01:26:43 GMT (Sat)

- > [This echoes what Peter Ladkin contributed to RISKS-15.30, and is
- > included for those of you who did not go through Peter's account. PGN]

I'm afraid I disagree that this echoes my account. Although Udo may have correctly reported what the TV said, I find the account misleading. I'd like to clarify some differences.

First, `causes': the final report from the Polish authorities will be *the* legally valid document enumerating the factors. The major players are all discussing their favored candidates, but there is not unanimity. At least one candidate factor mentioned in my article has not been reported yet by the media [RISKS is sometimes first!]. It was not on Udo's list, which is a strict subset of the candidates so far. There may be more that we're not aware of yet. Factor 3 reported by Udo is a misleading statement of the braking logic.

Udo reports that Airbus 'agreed to modify its control system'. I wonder. The so-called 'modification' has been available as an option to operators for some time, and has been installed on delivered A320s. Airbus has already noted that this option is available to operators. This can't count as modification.

Peter Ladkin

★ Reminder for DCCA-4: Fourth IFIP Working Conference

Flaviu Cristian <flaviu@cs.ucsd.edu> Fri, 03 Dec 1993 17:37:39 -0800

[For a full copy of the program and registration information, send E-mail to Flaviu Cristian <flaviu@cs.ucsd.edu> or dcca@cs.ucsd.edu or fax to +1-619-534-7029, or a telephone call to Keith Marzullo, +1-619-534-3729. An earlier version, with that information, is in RISKS-15.05. PGN]

DCCA-4: Fourth IFIP Working Conference on Dependable Computing for Critical Applications January 4-6, 1994 Catamaran Resort Hotel, San Diego, California, USA

Organized by the IFIP Working Group 10.4 on Dependable Computing and Fault-tolerance, in cooperation with:

IFIP Technical Comittee 11 on Security and Protection in Information Processing Systems

IEEE Computer Society Technical Committee on Fault-tolerant Computing EWICS Technical Committee 11 on Systems Reliability, Safety and Security University of California at San Diego

ADVANCE PROGRAM

Monday, January 3, 7-10pm Welcome Reception

Tuesday, January 4
9:00-9:15am Opening Remarks
F. Cristian, General Chair

G. Le Lann, T. Lunt, Program Co-chairs

9:15-10:45am Session 1: Formal Methods for Critical Systems
Chair: M. Melliar-Smith (U of California, Santa Barbara, US)
W. Turski, Warsaw University, Poland: On Doubly Guarded
MultiprocessorControl System Design
G. Bruns, S. Anderson, U of Edinburgh, UK: Using Data Consistency
Assumptions to Show System Safety

11:00-12:30am Panel Session 1: Formal Methods for Safety in Critical Systems Moderator: Ricky Butler (NASA Langley, US)
Panelists: S. Miller (Rockwell Collins, US), M. J. Morley (British Rail/Cambridge, UK), S. Natarajan (SRI International, Menlo Park, US), F. Schneider (Cornell U, US).

1:30-3:00pm Session 2: Combining The Fault-tolerance, Security and Real-time Aspects of Computing

Chair: C. Landwehr (NRL, Washington DC, US)

P. Boucher et al, SRI Intl, US: Tradeoffs Between Timeliness and Covert Channel Bandwith in Multilevel-Secure, Distributed Real-Time Systems

K. Echtle, M. Leu, Dortmund U, Germany: Fault-Detecting Network Membership Protocols for Unknown Topologies

4:00-6:00pm Session 3: Secure Systems

Chair: P. G. Neumann (SRI International, Menlo Park, US)

- J. Millen, MITRE: Denial of Service: A Perspective
- R. Kailar, V. Gligor, S. Stubblebine: U of Maryland, US: Reasoning About Message Integrity
- R. Kailar, V. Gligor, U of Marland, L. Gong, SRI: On the Security Effectiveness of Cryptographic Protocols

Wednesday, January 5

9:00-10:30am Session 4: Assessment of Dependability

Chair: W. Howden (U of California, San Diego)

- C. Garrett, M.Yau, S. Guarro, G. Apostolakis, UCLA, US: Assessing the Dependability of Embedded Software Systems Using the Dynamic Flowgraph Methodology
- A. Aboulenga, TRW and D. Ball, MITRE, US: On Managing Fault-tolerance Design Risks

11:00-12:30 Panel Session 2: Qualitative versus Quantitative Assessment of Security

Moderator: T. Lunt (SRI International, Menlo Park, US)

Panelists: M. Dacier (LAAS, Toulouse, France), B. Littlewood (City U, London, UK), J. McLean (NRL, US), C. Meadows (NRL, US), J. Millen (MITRE, US)

1:30-3:00pm Session 5: Basic Problems in Distributed Fault-tolerant Systems Chair: F. B. Schneider (Cornell U, Ithaca, US)

C. Walker, M. Hugue, N. Suri, Allied Signal Aerospace, US: Continual On-Line Diagnosis of Hybrid Faults

A. Azadmanesh, R. Kieckhafer, U of Nebraska, US: The General Convergence Problem: A Unification of Synchronous and Asynchronous Systems

4:00-6:00pm Session 6: Specification and Verification of Distributed Protocols Chair: R. Schlichting (U Arizona, Tucson, US)

- O. Babaoglu, U of Bologna, Italy, M. Raynal, IRISA, France: Specification and Verification of Behavioral Patterns in Distributed Computations
- P. Zhou, J. Hooman, Eindhoven Univ, The Netherlands: Formal Specification and Compositional Verification of an Atomic Broadcast Protocol
- H. Schepers, J. Coenen, Eindhoven Univ, The Netherlands: Trace-Based Compositional Refinement of Fault-Tolerant Distributed Systems

6:30-10pm: Banquet; after dinner speaker: P. G. Neumann, SRI Int, US

Thursday, January 6

9:00-10:30am Session 7: Design Techniques for Robustness

Chair: J. Meyer (U. Michigan, Ann Arbor, US)

- N. Kanawati, G. Kanawati, J. Abraham, U of Texas, US: A Modular Robust Binary Tree
- R. Rowell, BNR, V. Nair, SMU, Texas, US: Secondary Storage Error Correction Utilizing the Inherent Redundancy of Stored Data

11:00-12:30 Panel Session 3: Common Techniques in Fault-Tolerance and Security

Moderator: C. Levitt (U of California, Davis, US)

Panelists: Y. Deswartes (LAAS, Toulouse, France), C. Meadows (NRL, US)

P. G. Neumann (SRI International), B. Randell (U of Newcastle upon

Tyne, UK), K. Wilen (U of California, Davis, US)

1:30-3:00pm Session 8: Real-Time Systems

Chair: L. Sha (SEI, Pittsburgh, US)

- M. Goemans, I. Saias, N. Lynch, MIT, US: A Lower Bound for Faulty Systems without Repair
- S. Ramos-Thuel, J. Strosnider, CMU, US: Scheduling Fault Recovery Operations for Time-Critical Applications

4:00-6:00pm Session 9: Evaluation of Dependability Aspects

Chair: K. Trivedi (Duke U, Durham, US)

- G. Miremedi, J. Torin, Chalmers Univ, Sweden: Effects of Physical some Software Implemented Error Detection Techniques
- J. Dugan, Univ of Virginia, M Lyu, Bellcore, US: System-Level Reliability and Sensitivity Analysis for Three Fault-Tolerant System Architectures
- J. Carrasco, U Polit de Catalunya, Barcelona, Spain: Improving Availability Bounds Using the Failure Distance Concept

CONFERENCE ORGANIZATION

General Chair: F. Cristian, U of California, San Diego, USA

Program Co-chairs: G. Le Lann, INRIA, France, T. Lunt, SRI International, USA Local Arrangements/Publicity Chair:K. Marzullo, U of California, San Diego, USA



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 33

Tuesday 7 December 1993

Contents

- Review: "Digital Woes" by Lauren Ruth Wiener **Pete Mellor**
- Review: "Terminal Compromise" by Winn Schwartau **Rob Slade**
- Info on RISKS (comp.risks)

Review: "Digital Woes" by Lauren Ruth Wiener

Pete Mellor <pm@csr.city.ac.uk> Tue, 7 Dec 93 18:44:00 GMT

Title: Digital Woes

Subtitle: Why we should not depend on software

Author: Lauren Ruth Wiener

Publisher: Addison-Wesley Publishing Company

ISBN: 0-201-62609-8 Price: US \$22.95 245 pages, hardback

This is a highly entertaining and easily readable book on a subject which is dear to all our hearts. Without stretching the technical knowledge of the average reader in the slightest, the author has managed to present a comprehensive account of the problems that beset modern software-based systems.

She sets the scene in "Attack of the Killer Software", by presenting 13 incidents in which disaster was caused, or nearly caused, by the misbehaviour of software, including Mariner 1, Apollo 11, the Patriot's Scud-chasing problems, the Bank of New York glitch, Therac-25, the ozone-layer fiasco, and a few others.

If these sound familiar to readers of RISKS, this is no coincidence. The majority of the raw material was taken from its archives, so providing a handy counter-example of the sensible use of computing equipment.

Chapter 2 "Why Does Software Have Bugs?" describes the basic causes of the "Software Crisis" (except that the author points out in her conclusions that there is really no such thing: it is simply in the nature of software to contain bugs). I had a strong feeling of "deja vu" reading this chapter, mainly because it would make a good set of revision notes for the 1st-year undergraduates on the Software Engineering course that I teach. The author describes very well the discontinuity of behaviour that makes digital systems so treacherous compared to more conventional analogue systems. She makes the points that software is always part of a larger system, and so subject to the vagaries of the system environment, that it suffers from complex execution paths, timing problems (which make it truly non-deterministic), and unforeseen interactions due to its high level of connectivity in distributed systems. (These latter problems are well illustrated with reference to the AT&T collapse of 1990.) The problems of novelty of design and the lack of engineering discipline as applied to software (at least until recently) could possibly have been given more attention, and it would have been good to see the concept of programming as a subtractive exercise developed at greater length.

The problem of resources is the subject of Chapter 3. This kicks off with the classic 1979 US GAO study of 9 Federal Projects, and then goes on to demonstrate that not much has changed, using a table of remarks quoted from a 1967 article in Fortune magazine set against similar statements from later papers and articles from 1971 to 1991. Problems arising from the development organisation (corporate hierarchies are not ideal organisational structures for creating software), from the development process (getting the requirements right, design, development, testing, "gutless estimation" of effort and schedule and the resulting overruns), what passes for "maintenance" of software, etc., are well covered, along with the value of prototyping, and an account of the kind of "warranties" traditionally offered by software vendors (i.e., disclaimers!).

Safety-critical systems are the subject of Chapter 4, with an account of the applicable software engineering techniques, including the use of software standards, formal specification and mathematical verification. The author is not hopeful that any of these methods can "deliver the goods". Software standards are more honoured in the breach than in the observance. There is the eternal problem of whether to mandating aspects of the development process or the resulting product. There is on evidence that the stipulated techniques actually result in safer systems. (Indeed, some standards may be counter-productive.) Formal specifications are difficult to write and usually the domain experts cannot understand them. These problems have led (for example) to Boeing specifying the 777 flight control system in English. Proof of correctness is even more arduous and expensive, and may not detect specification faults. The author cites the classic paper by De Millo, Lipton and Perlis in support of these arguments, as well as the unhappy experience of Ontario Hydro in attempting to prove one of their reactor shut-down systems correct. Several formal methods specialists are quoted to the effect that formalism alone is insufficient.

Certifying software engineers to work on safety-critical systems offers no easy solution either, due largely to the lack of consensus on what core curriculum should be studied in order to qualify. The main effect of requiring

certified personnel will be increased cost of software (and it will still have bugs!).

The rest of the chapter introduces the basic concepts of risk analysis, including HAZOP, FMEA, FTA, etc., and discusses the use of redundancy and planned failure paths in fault-tolerant systems, so that they can "fail-safe" or "fail-soft". The author points out that, paradoxically, it is often the "safety" features of a system that lead to disaster.

The author next deals with something that probably does not get the attention it deserves as a topic in its own right in the average Software Engineering course. This is the temptation to "think big" where software systems are concerned, partly due to their ease of connection (since they are all digital). Chapter 5 discusses the issues of connectivity at length, the use of communications networks of various kinds (particularly multi-media), "data as a commodity" and the attendant risks to privacy (e.g., from the misuse of distributed databases) and other social implications of digital technology. Distribution is cheap - security is expensive. The fact that digital information is volatile raises various questions of authenticity. What is the value of a digitised signature? Which version of an electronic book is an author's genuine work? How can electronic voting affect the democratic process? (Answer: badly!) Is a digitally recorded video admissible as evidence in court, or could it have been skilfully forged? How do computer generated simulations of an accident influence a jury?

The tendency to do everything-"by-wire" is well covered (fly-, sail-, drive-, etc.) and the opportunity this provides for the introduction of massive control systems, such as GPS navigation, the Advanced Automation System for air traffic control, and the proposals for even more radical Advanced Vehicle Control Systems running "platoons" of cars at 90mph with 10 inches separation between the bumpers. Needless to say, the author is less than enthusiastic about most of these proposals. In the meantime, Thailand is setting up a central database to record all essential information about all of its 55 million inhabitants, and has received an award from the Smithsonian for its efforts.

In the final chapter the author summarises her argument and proposes seven questions that we should ask about any proposed system, starting with "Do we need it?". We should counterbalance the enthusiasm for big technical projects by asking: "Is it the right system?", "What is at risk when (not if) it goes wrong?", "How big and complex will it have to be?", "How will it fit in with what already exists?", "What will it require of its users?", "Will it require extensive security?", "Is there a back-up?".

She also makes two "modest proposals" for projects which would be a sensible use of resources: the "Educational Software Foundation" and "Congress On-line". The first would inject funds into the exploitation of computing power to educate children, taking advantage of the possibilities of interactive graphical systems and virtual reality. The second would decentralise Congress, so that the lawmakers could live among their constituents, and conduct business by computer bulletin board. Washington, D.C., would be redundant: no more big expenses, no crowds of fat-cats lobbying for big corporations! (The only slight objection I had here was that lobbying

by e-mail would be just as easy as law-making by e-mail.)

I do not know how much computers are already available in US schools, but certainly many schools in the UK are making good use of them at all levels of primary and secondary education, thanks largely to the imaginative initiative by the BBC in conjunction with Acorn. There is also the Nuffield mathematics project. Of course, the use of computers is uneven, as is funding for other aspects of education.

Trying to place the second proposal in a UK context, I was unable to imagine many British MPs being willing to give up their perks (not to mention the opportunity for a bit of toe-sucking on the quiet! :-) for a life in front of a computer terminal in the Orkneys. The Lords Spiritual and Temporal would presumably have to find another way of justifying their daily attendance allowance, and I doubt that logging in to read their e-mail would suffice. Precisely how the Queen's speech would be handled, and what the electronic equivalent of Black Rod would be, I leave to more imaginative readers! :-)

As will be seen from this synopsis, the author's tone is sceptical throughout. She has little patience with misplaced enthusiasm for grandiose schemes in the field of IT. One by one, they all take a hammering; in some cases, such as the Strategic Defence Initiative, several hammerings. Most of the well-known software disasters of recent years make their appearance at some point. The author's message is that we have choices about what systems we implement, that these choices will fundamentally affect the quality of our lives, and should be made with our eyes open to the disadvantages as well as the potential gains.

As a step in educating the lay public in the social issues of information technology, the book is excellent, and should be required reading in any foundation course on software engineering, or any course with a title such as "Computers and Society".

The level of difficulty is just about right for the non-technical reader. The style is witty and the pace is maintained. At the same time, the book is scholarly, and all technical points or disaster stories in the text are supported by notes and references at the end of each chapter. The specialist reader will find it useful as a source of references to more technical descriptions.

There is a glossary of computing terms with some good explanations. The definition of a "system" as a "set of systems ..." in order to emphasise its recursive nature struck me as being particularly neat. The remark in the definition of "natural language" that (because of the difficulty of teaching natural language to a computer) "It is hard to avoid the conclusion that children have special wiring." is a nice example of the humour of the book.

As far as I could judge, the descriptions of disasters are accurate. The author avoids urban myths (e.g., she gives a good account of the loss of Mariner, on which misleading information is extremely persistent). There are technical inaccuracies, however.

The author is wrong in several places about my favourite aeroplane. For

example (p.17), the Airbus which was downed as a result of the Vincennes' crew's inability to read a timetable fast enough, and Aegis' inability to report whether it was climbing or descending, was either an A300 or an A310, but definitely not an A320. Software (p.25) does *not* take the place of the hydraulics on the A320 and other aircraft of its generation. The control surfaces are still (mostly) moved hydraulically, although the signals to the hydraulic actuators are electrical, and are output by the computers in the Electrical Flight Control System (EFCS). (This mistake is repeated on p.87.) She also confuses the functions of the EFCS and the Flight Management and Guidance System in the same paragraph.

The end-of-chapter note states that on the A320, there is one small control surface on each wing under the pilot's direct control. This might have come from the reference cited (Stix, Gary: "Along for the Ride?", Scientific American, July 1991, pp. 94-106), but in any case it is wrong. The "manual back-up" in the event of total EFCS failure consists of pitch control by movement of the Trimmable Horizontal Stabilizer using the trim wheels, and control of direction using the rudder, which can be moved directly by pedals.

In some places, the need to address a lay audience has led to oversimplification of a technical point. For example, in the discussion of fly-by-wire (p.88), it is stated that the "safe flight envelope" is defined as "the limits of structural integrity of the aircraft". There is lot more to it than that.

The description of the Shuttle computer architecture on p.30 is a bit confusing, and is not helped by the use of "operational" where what is meant is obviously "fail-operational". Also, I was left wondering if "fail-safe" and "fail-operational" had been applied correctly.

The description of digital representation on p.44 is confused by the fact that the binary pattern "0100011" is mistakenly described as the representation of the number "67" instead of "35".

Analogue images (p.154), like digital images, possess only finite resolution.

Just to be really pedantic, I doubt that Augusta Ada Byron, Countess of Lovelace, ever referred to herself as "Ada Lovelace" (p.16)! :-)

I found myself objecting to one or two of the definitions. I have always understood a "patch" to be a modification to executable code, not a hasty modification to source code. Also a "bug" is defined as "Behaviour on the part of a computer program ..." and "failure" as "An inability of some part of a system ...". The standard usage is that a "bug" is a "latent fault", i.e., a *state* of the system, and a "failure" is an *event* in which a system does not perform a required function (one of the causes of which may be the "activation" of a bug).

A glossary of acronyms would be a useful addition. I could only guess from the context that "UPS" is a parcel delivery service, and the only words I could attach to "VPL" were "Visible Panty Line", though this might have been due to the proximity of a passage describing the potential pornographic uses of virtual reality! :-)

These minor criticisms do not detract from the overall value of the book.

To the author's two "modest proposals" in Chapter 6, I would like to add a third of my own. Before the number of safety-critical software-based systems exceeds the number of inhabitants of Thailand, could we not set up a central database (either one international one, or several national ones) on which to register these and record their dependability in service? To those who object to the effort involved, I would say: how much effort did it take to register every computer in the UK which holds confidential personal information, as required by the Data Protection Act? Are we prepared to do as much to protect our safety as to protect our privacy?

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB Tel: +44 (71) 477-8422, Fax.: +44 (71) 477-8585, E-mail (JANET): p.mellor@csr.city.ac.uk

Review: "Terminal Compromise" by Winn Schwartau

"Rob Slade, Ed. DECrypt & ComNet, VARUG rep." <roberts@decus.arc.ab.ca> 4 Dec 93 23:58 -0600

BKTRMCMP.RVW 931002

Inter.Pact Press 11511 Pine St. N. Seminole, FL 34642 813-393-6600

fax: 813-393-6361

"Terminal Compromise", Schwartau, 1991, 0-962087000-5, U\$19.95/C\$24.95 wschwartau@mcimail.com p00506@psi.com

"Terminal Compromise" was first published in 1991, and was enthusiastically promoted by some among the security community as the first fictional work to deal realistically with many aspects of data communications and security. Although still available in that form, recently is has been "re-issued" in a softcopy "shareware" version on the net. (It is available for ftp at such sites as ftp.uu.net, ftp.netsys.com, soda.berkeley.edu and wuarchive.wustl.edu. Use archie to look for TERMCOMP.) Some new material has been added, and some of the original sections updated. Again, it has been lauded in postings on security related newsgroups and distribution lists.

Some of you may be old enough to recall that the characters current in "Outland" sprang from a previous Berke Breathed cartoon strip called "Bloom County". Opus, at one point, held the post of movie reviewer for the "Bloom County Picayune". I remember that one of his reviews started out, "This movie is bad, really bad, abominably bad, bad, bad, bad!" He considers this for a moment, and then adds, "Well, maybe not *that* bad, but Lord! it wasn't good!"

A fairly large audience will probably enjoy it, if such trivialities as language, characterization and plot can be ignored. For once the "nerds"

don't get beat on; indeed, they are the heroes (maybe). The use of computers is much more realistic than in most such works, and many ideas that should have greater currency are presented. The book will also appeal to paranoiacs, especially those who believe the US federal government is out to get them.

Consistency is the hobgoblin of little minds -- but it does make for a smoother "read". "Terminal Compromise" would benefit from a run through a style checker ... and a grammar checker ... and a spelling checker. Constructions such as "which was to be the hypocenter of the blast if the Enola Gay hadn't missed its target" and "National Bureau of Standards which sets standards" are understandable, although awkward. In other places it appears words might be missing, and you have to read over sentences several times to puzzle out the meaning. (The softcopy/shareware version comes off a little worse here, with fragments of formatting codes left in the text.)

On second thought, forget the spelling checker. Most of the words are spelled correctly: they are simply *used* incorrectly. A reference to an "itinerant professional" has nothing to do with travelling. (Maybe he meant "consummate": I couldn't think of a synonym starting with "i".) The "heroine" trade was probably intended to refer to white powder rather than white slavery. There are two automobile "wreak"s. "Umbrage" is used twice. An obscure seventeenth century usage did once refer to shelter given by islands to a harbour, but it's stretching the language a bit to make it refer to a covering for the naughty bits. Umbrage usually refers to offence, suspicion, doubt or rage, as in "I take umbrage at what I suspect is a doubtful use of the language".

Characterization? There isn't any. The major characters are all supposed to be in their forties: they all, including the President of the United States, speak like unimaginative teenage boys whose vocabulary contains no adjectives other than obscenities. This makes it difficult at times to follow the dialogue, since there are no distinctives between speakers. (The one exception is the president of a software firm who makes a successful, although surprising, translation from "beard" to "suit", and is in the midst of the most moving and forceful speech in the book, dealing with our relationship to computers, when the author has him assassinated.)

The book is particularly hard on women. There are no significant female characters. None. In the initial introduction and background of the hero there is no mention of a significant other. It is something of a shock later to discover he is married, then that he is divorced. Almost all of the females are simply bedroom furniture. The portrayals remind one of the descriptions in "Don Quixote" of women "so gay, striking and beautiful that the sight of her impressed them all; so vividly that, if they had not already seen [the others], they would have doubted whether she had her match for beauty".

Which raises another point. All of the hackers, except some of the Amsterdam crew, are fit, athletic and extremely attractive to the female of the species. Even among the I-Hack crowd, while there may be some certifiable lunatics, nobody is unkempt or unclean. These urbane sophisticates drink "Glen Fetitch" and "Chevas" while lounging in "Louis Boston" suits on "elegant ... PVC furniture". Given that the hackers save the day (and ignoring, for the moment, that they caused the trouble in the first place) there seems to be

more than a touch of wish fulfillment involved.

(Schwartau tries to reiterate the "hackers aren't evil" point at every opportunity. However, he throws away opportunities to make any distinctions between different types of activities. Although the different terms of phreaks, hackers and crackers are sprinkled throughout the story they are not well defined as used by the online community. At one point the statement is made that "cracking is taking the machine to its limit". There is no indication of the divisions between phreaks, hackers and crackers within their various specialties, nor the utter disdain that all three have for virus writers. Cliff Stoll's "Hanover (sic) Hacker", Markus Hess, is described as a "well positioned and seemingly upstanding individual". This doesn't jibe with Stoll's own description of a "round faced, slightly overweight ... balding ... chain smoking" individual who was "never a central figure" with the Chaos Computer Club, and who, with a drug addict and a fast buck artist for partners "knew that he'd screwed up and was squirming to escape".)

What little character is built during the story is unsteady. The author seems unable to decide whether the chief computer genius is one of the good guys or the bad. At times he is mercenary and self-centred; at others he is poetic, eloquent and visionary; in yet other scenes he is mentally unbalanced. (He also appropriates the persona and handle of another hacker. We are never told why, nor are we ever informed of what happened to the original.) Following the characters isn't made any easier by the inconsistency of naming: in the space of five paragraphs we find that our hero, Scott Byron Mason (maybe) is the son of Marie Elizabeth Mason and Louis Horace Mason. Or possibly Evelyn Mason and Horace Stipton Mason. The main academic studying viral programs is Dr. Les (or Arnold) Brown (or Sternman) who is a professor at Sheffield (or MIT). (Interestingly, there is an obvious attempt to correct this in the later "softcopy" version of the book. At times the "corrections" make the problem worse.)

For a "thriller", there is very little tension in the story. The unveiling of the plot takes place on a regular step by step basis. There is never any hint that the hero is in the slightest personal danger: the worst that happens is that one of his stories is quashed. Indeed, at the end of the book the computer attacks seem basically all to have succeeded, credit card companies are bankrupt, banks are in a mess, airlines are restricted, phone systems are unreliable and the bad guys are in charge. Yet our heroes end up rich and happy on an island in the sun. The author seems to be constantly sounding the alarm over the possibility of this disaster, but is unwilling, himself, to face the tremendous personal suffering that would be generated.

Leaving literary values aside, let us examine the technical contents. The data security literate will find here a lot of accurate information. Much of the material is based on undisputed fact; much of the rest brings to light some important controversies. We are presented with a thinly disguised "Windows", a thinly disguised Fred Cohen (maybe two?), a severely twisted Electronic Freedom Foundation, and a heavily mutated John Markoff. However, we are also presented with a great deal of speculation, fabrication and technical improbabilities. For the technically adept this would be automatically disregarded. For the masses, however (and this book seems to see itself in an educational light), dividing the wheat from the chaff would

be difficult if not impossible.

As with names, the author appears to have problems with the consistency of numbers. In the same paragraph, the softcopy version has the same number quoted as "over 5000", "almost 5000" and "three thousand". (It appears to have been "corrected" or updated from the original version without reading the context). A calculation of the number of hackers seems to be based upon numbers pulled out of the air, and a computer population an order of magnitude larger than really exists. The "network", seemingly referring to the Internet, has a population two orders of magnitude too large. Four million legal copies, with an equal number of pirate copies, of a virus infected program apparently result in only "between 1 and 5 million" infections. (I *knew* a lot of people had bought Windows but never used it!) Not the most prolific virus we've ever seen.

Schwartau seems uncertain as to whether he wants to advertise real software or hide it. At various times the characters, incessantly typing to each other across the (long distance) phone lines use "xtalk" (the actual filename for Crosstalk), "ProCom" (ProComm, perhaps?), "ComPro" and "Protalk". They also make "4800 BAUD" connections (technically unlikely over voice grade lines, and even if he meant "bits per second" 4800 is rather an odd speed) and communicate with "7 bits, no parity, no stop bits" parameter settings. (The more common parameter settings are either 8 bits, no parity or 7 bits, even parity. You *must* have stop bits, usually one. And to forestall the obvious criticism, there is no indication in the book that a "non-standard" setting is being used for security reasons.)

We are, at places in the text, given detailed descriptions of the operations of some of the purported viral programs. One hides in "Video RAM". Rather a stupid place to hide since any extensive video activity will overwrite it. (As I recall, the Proto-T hoax, which was supposed to use this same mechanism, started in 1991. Hmmm.) Another would erase the disk the first time the computer was turned on, which leads one to wonder how it was supposed to reproduce. (This same program was supposed to be able to burn out the printer port circuitry. Although certain very specific pieces of hardware may fail under certain software instructions, no printer port has ever been numbered among them.) One "hidden file" is supposed to hide itself by looking like a "bad cluster" to the system. "Hidden" is an attribute in MS-DOS, and assignable to any file. A "bad cluster" would not be assigned a file name and therefore would never, by itself, be executed by any computer system. We also have a report of MS-DOS viri wiping out a whole town full of Apple computers.

Schwartau is not averse to making up his own virus terminology, if necessary. ("Stealth" is also reported as a specific virus.) At one point the book acknowledges that viral programs are almost invariably detected within weeks of release, yet the plot relies upon thousands of viri remaining undetected for years. At another point the use of "radio broadcasts" of viral programs to enemy systems is advocated, ignoring the fact that the simplest error checking for cleaning "noise" from digital radio transmissions would eliminate such activity.

A number of respected security experts have expressed approval of "Terminal Compromise". This approbation is likely given on the basis that this book is so much better than other fictional works whose authors have obviously had no

technical background. As such the enthusiasm is merited: "Terminal Compromise" raises many important points and issues which are currently lost on the general public.

Unfortunately, the problems of the book, as a book, and the technical excesses will likely restrict its circulation and impact. As a fictional work the lack of literary values are going to restrict both its appeal and longevity. As an exhortative or tutorial work, the inability to distinguish between fact and fiction will reduce its value and effectiveness in promoting the cause of data security.

copyright Robert M. Slade, 1993 BKTRMCMP.RVW 931002

=========604-984-4067========

Vancouver Institute for Research into User Security Canada V7K 2G6 ROBERTS@decus.ca Robert_Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 34

Monday 13 December 1993

Contents

Computer glitch postpones 'Tommy'

David Tarabar

Electronic Money

Brian Randell

Financial Newswire Fraud

Thomas J Scoville

Canadian study on computer fraud

Mich Kabay

Risks of being a programmer

Jon Jacky

The risk of distributed servers with only partial uninterruptible power

Bob Cunningham

Risks of inband communication triggering call forwarding

Simson L. Garfinkel

Mail forwarding as easy as Call forwarding

Kiser

Re: Massive credit card fraud

Pete Mellor

Apple has poked around on your hard disk before

Grady Ward

Re: Corrupted Polling

Brian Randell

Re: Digital Woes

Harry Erwin

COMPASS '94 Call for Papers and Call for Tutorials

John Marciniak

Info on RISKS (comp.risks)

Computer glitch postpones 'Tommy'

David Tarabar <dtarabar@hstbme.mit.edu> Fri, 3 Dec 93 18:51:16 -0500

From the Boston Globe of Friday, 3 Dec 1993:

What "The Who's Tommy" needed yesterday was a computer wizard, not a pinball wizard. Last night's opening Boston performance of the high-tech musical was canceled because several computers required to stage the show suffered technical difficulties as a result of being shipped to the Colonial Theatre from Louisville, where the production completed a one-week run on Sunday. ... "Touring is apparently being more funky on the computers than anyone anticipated," David Balsom, the show's local press representative, lamented last night. ...

Electronic Money

<Brian.Randell@newcastle.ac.uk>
Fri, 10 Dec 1993 12:35:44 GMT

The attached article is from The Independent, 9 Dec 1993. This is the first I have heard of such a scheme here in the UK, but would not be at all surprised if similar schemes already exist elsewhere (you would not expect to find such information from a press conference!).

I was particularly "interested" in the paragraph:

The key to the card's security lies in the Japanese-developed technology and microchip. NatWest and Midland said that a technical breakthrough had made it impossible to counterfeit cards.

and look forward to the reactions of RISKS' readers.

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

TIME FOR A TOP-UP: MONDEX FACES A YEAR-LONG TRIAL, BEGINNING IN SWINDON IN 1995.

NATWEST IS RUNNING THE PROJECT IN CONJUNCTION WITH MIDLAND AND BRITISH TELECOM.

BANKS STEP UP WAR ON CASH WITH PLASTIC CARD THAT CAN BE TOPPED UP BY PHONE

EVEN STREET VENDORS WILL BE ABLE TO TAKE THE NEW ELECTRONIC MONEY, SAY ITS MAKERS.

Nicholas Bannister reports on Mondex

NATIONAL Westminster Bank has developed an alternative to cash - a plastic card with a microchip which stores "electronic money" and can be topped up over the phone. Yesterday it revealed plans for a year-long trial of Mondex, its electronic money system, starting in Swindon in 1995. The pilot project, in conjunction with Midland Bank and British Telecom is likely to involve about 10,000 people, mainly bank customers and retailers.

The system lets customers add money to their card by using adapted cash dispensers or phones to access their accounts. Once charged with money, the card becomes the equivalent of cash. Payments are made by slipping the card into a retailer's terminal. The sum is transferred from the card to the retailer without need for time-consuming authorisations or signatures. Provided there is enough money on the card, the transaction will take place.

Payments between individuals are carried out by inserting the card into a pocket-sized electronic wallet and making six keystrokes. Both customers and retailers can deposit electronic money into their bank accounts over the phone.

Bert Morris, NatWest's deputy group chief executive, said that cash was still used for 90 per cent of all transactions in the United Kingdom, and that handling cash cost the banks more than #4.5 billion a year. He claimed that widespread use of Mondex would not lead to staff cuts and branch closures. Mr Morris, who is also on the Department of Social Security board, said that social security fraud could be reduced if the Mondex system was used for payments.

Tim Jones, one of the two NatWest executives who came up with the Mondex concept, said the card was not intended to replace traditional debit and credit cards. The system was designed for small and large payments. Small traders, for example a newspaper vendor, could have a battery-powered terminal. He claimed that it was safer, quicker and more convenient to handle electronic rather than physical money. But if a Mondex card was lost or stolen, the money on it would be lost in the same way as money in a missing wallet.

However, cards could be locked to prevent unauthorised use by tapping in a four-digit personal code. Once locked, the money could not be spent without re-entering the code. He said initially cash dispensers would be adapted to give customers the choice between drawing physical or electronic money. But the telephone would be the most important access point.

BT was planning to adapt its pay phones, and special phones for home use were being designed. Customers would insert the card into the phone triggering an automatic call to the bank's computer system. After a prompt, the customer would tap in his personal identification number and transfer money from his account to the card or vice-versa. "Our strategy is that in 10 to 15 years time, we will see the phone as the dominant way in which electronic money is drawn and deposited," Mr Jones said.

Derek Wanless, NatWest's chief executive, said: "Although Mondex will be launched in the UK, it is a major commercial, opportunity for banks everywhere. Mondex is a multi-currency product, capable of holding five separate currencies on a card simultaneously." He said that other British and foreign banks would be invited to join Mondex in due course to create a "truly global payment scheme". The British Retail Consortium said that the convenience, security, flexibility and potential for development should ensure customer acceptance of Mondex. Its director general, James May, said: "If successful, the Mondex trial should give UK shoppers a better way of paying, and provide retailers with benefits in this first step towards a cashless

society."

The key to the card's security lies in the Japanese-developed technology and microchip. NatWest and Midland said that a technical breakthrough had made it impossible to counterfeit cards. But Mr Jones said that Mondex would have a research budget "for ever" to keep ahead of the counterfeiters.

Financial Newswire Fraud

Thomas J Scoville <tscovill@world.std.com> Sun, 12 Dec 1993 14:55:56 -0500

Notes From the Financial Sector of Cyberspace: How To Profit by Faking Out the Market.

A good deal has been written lately on the ease, dangers, and risks of spoofing (or counterfeiting) mail on the net. Stories of practical jokes and character assassination abound. A similar but much more serious risk exists in financial information networks.

My consulting work brings me in touch with some very large mutual fund companies. Many of them have extensive network infrastructure to support systems to quickly distribute news items from a variety of sources: Comtex, Dow-Jones, Standard&Poors, and others.

The delivery end of these systems work like a cross between rn and a mail-reader: Story headlines are displayed (like mail "Subject:" lines), most recent to least, with the body of the news story available on demand. The headlines are constantly updated with fresh stories.

The news service is used by a variety of people: traders, portfolio managers, commercial brokers, to name a few. Trading (sometimes very high-volume trading) is quickly initiated based on the incoming news. Often the body of the stories is never read; hot stories contain only a headline - if you take the time to read the story, you've lost some or all of your opportunity.

The time-dependence of the incoming news is striking. The traders act immediately on the incoming information; their 'edge' is the timeliness of the news. It enables them to exploit short-lived opportunities. In that business, information goes stale and becomes useless very quickly, sometimes in a matter of minutes. The news source is trusted. Verifying stories is not a top priority.

With the proper access to the hub machines and a little understanding, news stories can be faked. Just as email can be spoofed with the popular port 25 Unix hack, a story which didn't originate at a legitimate news source can be injected into the flow. Given that the news wire is the trader's primary window into the marketplace, one could create a phantom in that window, one with predictable effects: "Bill Gates Dies of Heart Attack"... (perhaps just prior to selling short on Microsoft).

Now the risky part: my experience to date is that many of the hub machines,

servers, and subnets involved are no more secure than any on the Internet, and in some cases much less so. Any Unix site administrator connected to the Internet should be shivering in his/her boots at this point...

Tom Scoville - tscovill@xs.com

Canadian study on computer fraud

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 05 Dec 93 11:18:53 EST

>From United Press International newswire via Executive News Service (GO ENS) on Compuserve:

Study says database breaches costly and increasing, by Robb Stewart TORONTO (UPI, 2 Dec 1993) - A Canadian study released Thursday says one quarter of North American companies have suffered data base breaches, at a cost of up to \$1,000,000 per incident. The study by the Ernst and Young financial consulting firm and Information Week magazine said the problem is growing and that companies need to put greater emphasis on protecting their computer systems."

Key points:

- 30% of losses caused by employees.
- Half of these criminals are greedy, the rest disgruntled.
- o Organizations "must integrate system and date security into their basic information technology strategies" to reduce fraud.
- o 80% of all employees surveyed have access to computers.
- o Additional problems are caused by hackers and by natural disasters.
- o "...senior managers need to send a message to employees that this is a serious issue," according to the author, John Kearns.
- o The author emphasized the importance of employee awareness training, security policies, and especially the example set by senior managers. According to Kearns, "employees react to the attitude of senior managers, leaving PCs on, or leaving documents on their desk or sharing their password."

<

✓ Risks of being a programmer

Jon Jacky <jon@violin1.radonc.washington.edu> Mon, 13 Dec 1993 10:36:51 -0800

In this Sunday's NEW YORK TIMES (Dec. 12, 1993) the cover story on the

business section is about Apple's Newton handheld computer project:

MARKETER'S DREAM, ENGINEER'S NIGHTMARE

Apple's chief promised too much on the Newton, and the design team paid a heavy price. by John Markoff

... The pressure to finish, exhilarating at first, eventually overwhelmed some of the young designers. After 18-hour days, some engineers went home and cried. Some quit. One had a breakdown and ended up in jail. One took a pistol and killed himself.

(The story provides more detail on each of these.)

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

The risk of distributed servers with only partial uninterruptible power

"Bob Cunningham" <bob@kahala.soest.hawaii.edu> Fri, 10 Dec 93 07:08:48 HST

Earlier this year in the School of Ocean & Earth Science & Technology at the University of Hawaii we replaced our large centralized NFS servers (all in one building with a large-capacity uninterruptible power system) with small, distributed mini-servers on each subnet in each building.

This noticeably improved NFS performance, did away with a substantial amount inter-subnet network traffic, and reduced traffic significantly on the subnet the centralized servers were previously on. Economical, too, since the small servers were cheap. We didn't even bother to install UPS systems for the new mini-servers, though we did put the small server that replaced the large one in the original building on the old UPS. Which seemed like a good idea at the time...

Of course most of the services were duplicated on all servers and we crafted the NFS maps such that systems within a particular building mounted from their in-building NFS server if possible, but could use a server in another building if their local server was down.

Everything worked well until we had a series of power outages last week. After each outage, more and more individual computers would lock onto the small server in the original building (alway ups, thanks to its UPS) in preference to their local mini-server (with no UPS, those went down--and typically were slower to reboot than their former clients).

NFS mounts are remarkably tenacious. We finally had to shut down the UPS-protected mini-server for several hours and reboot a variety of systems in several buildings to relieve the single overloaded server.

Risks of inband communication triggering call forwarding

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Sat, 11 Dec 93 11:32:42 -0500

Fascinating article in the November 1993 issue of MIT Information Systems journal. "When Call Forwarding Goes Awry."

"Have you ever heard from people who tried to dial you directly at your MIT number, but got the MIT operator instead? Or the operator at the Whitehead Institute? Or someone with no connection with your department?"

Turns out that, at MIT, you can initiate a call-forwarding command by dialing 78-

Mail forwarding as easy as Call forwarding

<kiser@tecnet1.jcte.jcs.mil>
Tue, 7 Dec 93 23:56:53 EST

After a recent move, I decided to fill out a change-of-address form at the US Post Office to have my mail forwarded for me as my personal name, me as my sole proprietorship, both of the names of the little informal "businesses" I and each of two friends have formed (to be on better terms with larger companies), and, since each of my friends occasionally sends mail from our hobby/ventures to my place, for them as well (for a grand total of five forwarding orders).

I expected the large number of forwarding orders to be questioned; it wasn't. And I was not pleased to learn that just anyone can walk in and fill out one of these things for me. How did I come do that conclusion? I was not asked for any ID at all. Finally, when I asked if it "was ok" for me to fill out a change of address for someone else (i.e., the ones with my friends' names on them and my signature ;-<), the mail clerk responded "as long as they don't mind."

Has anyone ever tried to have 1600 PENNSYLVANIA AVENUE forwarded?

★ Re: Massive credit card fraud (RISKS-15.32)

Pete Mellor <pm@csr.city.ac.uk> Mon, 13 Dec 93 19:22:37 GMT

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> writes:

- > o Thieves monitor external mailboxes on homes for weeks in wealthy
- > neighbourhoods to steal credit cards and new cheques arriving in the
- > mail

A minor point here is that the theft requires the existence of *external* mailboxes, which are virtually unknown in the UK. (The only reason that UK e-mailers understand the "Mailbox" icon on the Sun windows interface is because they've read Li'l Abner! :-)

All "letterboxes" in the UK are slots in the front door with metal hinged flaps over them. The mail drops down inside and lands on the doormat. (One exception to this is that blocks of flats *sometimes* have downstairs mailboxes for all occupants, but these are usually opened only by the owner's key, and are usually in an internal foyer, with at least some protection from casual theft. I live in a high-rise block of flats, and the postman delivers mail to each individual flat.)

Risks here? Well, some terrorist or vandal could drop something nasty through it. (I will leave it to readers' imaginations what sort of "nasty" this could be!) Alternatively, the family dog could rip the mail to shreds. (This is a surprisingly common habit of dogs in the UK. I remember that the letterbox in my childhood home was backed by an internal mailbox to stop our otherwise sweet-tempered black labrador from doing just that.) Otherwise, the only problem is that delivery boys and postmen do not push the stuff right through the slot, so that a wedge of protruding paper advertises to the passing burglar that there is no-one at home, as well as leaving the mail itself once more vulnerable.

Given that the two problems above can be solved by simple devices or by training (of dogs and delivery boys!) there is a possible low-tech solution to high-tech crime (or aren't US postmen allowed to walk up garden paths? :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V OHB Tel: +44 (71) 477-8422, p.mellor@csr.city.ac.uk

✓ Apple has poked around on your hard disk before

Grady Ward <grady@netcom.com> Wed, 8 Dec 1993 09:32:47 -0800

Saul Tannenbaum in RISKS-15.32 explains how an uninvited software applet can unintentionally cause RISK to a user of certain Apple distribution software. This is not the first time that Apple software has violated the usual distinction between user hard disk data and its corporate interest.

In 1991 as part of their developer's CDROM, an Apple application automatically gathered information about your Macintosh system configuration, names of Inits, Cdevs, and Extensions (applets associated with the operating system and generally available to all applications).

Without assuring proper authorization, it then automagically e-mailed the information in real-time to Apple developer support. The RISK here is obvious: particular system configurations, code names of applications and system applets, and other gathered information could be used for significant competitive intelligence: knowing that the name of an application under development is, for example, NewApp version 1.0b32 gives a significant clue that the NewApp software is almost ready to go to market; knowing that a developer has installed a driver for a unique piece of hardware might very well tip off Apple that a new software product using that hardware is imminent.

Subsequent issues of the Developer's CDROM with he offending Hypercard stack were changed to make more explicit the default behavior of the intelligence-gathering trojan.

The RISK moral? A company has to give thought on how to obtain proper, informed authorization before a customer's privacy is invaded. :w

Re: Corrupted Polling, Inside Risks, Comm. ACM

<Brian.Randell@newcastle.ac.uk>
Fri, 10 Dec 1993 09:58:31 GMT

Quoting Rebecca Mercuri, Corrupted Polling, Inside Risks, Comm. ACM, vol 36, no 11, November 1993, p. 122.

>Technology alone does not eliminate the possibility of corruption and >incompetence in elections; it merely changes the platform on which they may >occur. The voters and the Election Boards who serve them must be made aware >of the risks of adopting electronic vote-tallying systems, insisting that >the checks and balances inherent to our democracy be maintained.

This comment reminds me of a fascinating book I read some years ago:

R.S. Brumbaugh. Ancient Greek gadgets and machines, New York, Crowell, 1966. (Reprinted 1975 by Greenwood Press, Westport, Conn.)

From memory, the author is a Professor of Classics, and puts forward the thesis that the Ancient Greeks tended to trust gadgets, i.e., physical devices, more than each other. He explains that this is why they devised and used, for example, means of trying to ensure that voting was carried out fairly, and that speeches were of equal length.

(Unfortunately the book is not readily available to me, otherwise I'd quote chapter and verse.)

[I think we are ready for Linux Polling. PGN]

Re: Digital Woes

Harry Erwin <erwin@trwacs.fp.trw.com> Wed, 8 Dec 93 15:11:58 EST

I just started this book, and it caused me to open my desk drawer where I had an old memo. This is a certificate of commendation for my participation and support on the BMDSTP Software Project during 1972-1979. If I may quote Jack Distaso:

Because of the expertise and dedication provided by the individuals who contributed to this project, STP established a record of outstanding performances which culminated with the complete success of the key demonstration mission for the Army. All milestones were completed on time, the software met 100 percent of its performance objectives, and the project

generated a substantial cost underrun on our incentive contract.'

My question is: why does this record remain nearly unique? My experience on the project seemed to show that software management was proactive and thorough. Since that time, I've never seen its like. The people on the project, while typically good-quality, were no better (for the most part) than many I've met since. What made the difference?

Harry Erwin herwin@cs.gmu.edu or erwin@trwacs.fp.trw.com

✓ COMPASS '94 Call for Papers and Call for Tutorials

JOHN MARCINIAK <marcinik@smtplink.cta.com> Fri, 03 Dec 93 16:20:24 EDT

CALL FOR PAPERS, COMPASS '94

9th Annual IEEE Conference June 27-30, 1994 on COMPuter ASSurance Gaithersburg, MD

The purpose of this conference is to bring together researchers, developers, and evaluators who work on problems related to specifying, building, and certifying high-assurance computer systems. What distinguishes COMPASS from similar conferences is its emphasis on bridging the gap between research and practice. Researchers are provided an opportunity to present results, new theories, and new technologies to both other researchers and practitioners who can put them to practice. They can also learn from practitioners of new research problem domains and of problems encountered in building real systems. Practitioners have an opportunity to share lessons learned, to learn of new research, and to influence future research.

Papers should present advances in the theory, design, implementation, evaluation, or application of high-assurance systems, or report on experiments, evaluations, and open problems in the use of new technologies for computer assurance. Special consideration will be given to presentations (either single papers or paper pairs) by practitioners and researchers who have worked on the same problem. There will also be a tools fair. Papers, panel session proposals, tutorial proposals, and tools fair proposals are solicited in the following areas:

Software Reliability Software Safety Computer Security Formal Methods Tools Process Models

Real-Time Systems Networks Embedded Systems

V&V Practices Certification Standards

INSTRUCTIONS TO AUTHORS:

Send five copies of your paper, panel session proposal, tutorial proposal, or tools fair proposal to John McLean, Program Chair, at the address given below. Abstracts, electronic submissions, late submissions, and papers that cannot be published in the proceedings will not be accepted. Papers submitted from outside North America should be sent via overnight courier service.

Papers must be received by January 15, 1994 and must not exceed 7500 words. Authors are responsible for obtaining prior to acceptance any and all necessary clearances for publication. Authors will be notified of acceptance by March 11, 1994. Camera-ready copies are due not later than April 22, 1994.

Papers that use technology presented at a previous COMPASS conference are eligible for a special award. Papers of exceptional quality and appropriate subject matter are eligible for inclusion in a special issue of the Journal of High Integrity Systems or the Journal of Computer Security.

Limited financial assistance will be available for student authors.

PROGRAM COMMITTEE

Paul Ammann, George Mason Univ; John Marciniak, CTA; George Dinolt, Loral; John McDermid, York Univ; Jan Filsinger, Booz-Allen Hamilton Jon Millen, Mitre; Virgil Gligor, Univ. of Maryland; John McHugh, Portland State U; Li Gong, SRI; David Parnas, McMaster Univ. Connie Heitmeyer, Naval Res. Lab; John Rushby, SRI; Jeremy Jacob, York Univ; Ravi Sandhu, George Mason Univ.; Carl Landwehr, Naval Res. Lab; Jeannette Wing, CMU; Teresa Lunt, SRI

FOR FURTHER INFORMATION CONCERNING THE SYMPOSIUM, CONTACT:

Jan Filsinger, General Co-Chair John McLean, Program Chair Booz-Allen Hamilton, Inc Naval Research Laboratory

8283 Greensboro Dr. Code 5543

Washington, DC 20375 Tel: (202)767-3852 Fax: (202) 404-7942

Fax: (703) 902-3131 filsing@itd.nrl.navy.mil

McLean, VA 22102

Tel: (703) 902-5302

mclean@itd.nrl.navy.mil

The COMPASS '94 Program Committee solicits your interest in presenting a tutorial at COMPASS '94.

The committee solicits tutorials that are pertinent to the goals of the conference and of interest to the attendees. We anticipate a full day of tutorials, the 27th of June 1994. This year we will offer an honorarium for the tutorial presentations.

Please submit your request to include the following information:

- 1. Topic and specific focus of the material
- 2. Length (1/2 and full day tutorials will be considered)
- 3. Name and background and experience in the area
- 4. Detailed topical outline

Selection will be made based on the appropriateness of the topic, the credentials of the presenter and the quality of the outline.

Schedule considerations:

Tutorials submissions: by 15 January, 1994

Response: by 1 February, 1994

Tutorial materials required: by 1 May 1994 *

Send requests to: John Marciniak, CTA, Inc., 6116 Executive Blvd

Rockville, MD 20852

301-816-1439 Fax: 816-1416 marcinik@smtplink.cta.com

* Tutorial materials will be required prior to the conference and will be subject to quality control procedures.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 35

Weds 22 December 1993

Contents

Airport lessons for InfoSec

Mich Kabay

Sham CD-ROMs

Mich Kabay

Smart Cars and Highways

Mich Kabay

Risky Demo Offer

Rex Wheeler

"Re-Chipping" Stolen Mobile Phones

Brian Randell

Interactive TV: electronic democracy, risks to privacy, etc.

John Gray

Trouble with funny place names

Mark Brader

Mexico Turns Off Quake Warning System

Frank Carey

Wireless Laptop Eavesdropping

Andrew Duane

Re: Harry Erwin on Digital Woes

Lauren Wiener

Question About Singapore Lottery Crime

Sanford Sherizen

ISOC Symposium on Network and Distributed System Security

Dan Nessett

Info on RISKS (comp.risks)

Airport lessons for InfoSec

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 14 Dec 93 05:48:02 EST

>From the Associated Press newswire through Executive News Service (GO ENS) on CompuServe:

Airport Security, By JAMES H. RUBIN (Associated Press Writer)

WASHINGTON (AP, 11 Dec 1993) -- Security is so poor at some of the nation's airports considered vulnerable to terrorists that federal investigators easily slipped past checkpoints and wandered around unchallenged.

The article goes on to state that investigators were rarely challenged as they walked through restricted areas even though they dressed informally and tried to draw attention to themselves. One agent successfully brought a grenade through metal detectors and inspection procedures. The inspectors often saw other unauthorized people in restricted zones.

Apparently security regulations are not taken seriously at many airports; there are few if any consequences for breaches of security.

Although this story has nothing to do with computer security, I cite it as yet another example of how important human factors are to security in general. Management must take security (including information security) seriously and apply rewards for compliance and punishment for failures. Employees need security awareness training and security drills. I would like to see intrusions as a normal part of security testing.

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

✓ Sham CD-ROMs

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 14 Dec 93 05:48:35 EST

>From the United Press International newswire via Executive News Service (GO ENS) on CompuServe:

Woman indicted in CD-ROM scam

SAN JOSE, Calif. (UPI, 10 Dec 1993) -- Federal officials said Friday a grand jury has indicted a San Jose woman for allegedly importing more than 900 counterfeit CD-ROMs from Hong Kong with the intent to sell them in the United States. U.S. Attorney Mike Yamaguchi said an indictment for software piracy had been handed down against Clare Waioi Sham, 29, of San Jose, and her company, C-88 International Corp.

The article mentions that this is the first software theft indictment involving CD-ROMs.

Personally, I think the best part of this story is that the person accused of preparing to sell counterfeit CD-ROMs is named "Sham."

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

Smart Cars and Highways

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 14 Dec 93 05:47:43 EST

>From the Washington Post newswire, 12 Dec 1993, through Executive News Service (GO ENS) on CompuServe:

Smart Car 54, Where Are You?; Washington's Latest Billion Dollar Boondoggle: Does Anyone Care? (By Marcia D. Lowe)

COMPUTER-EQUIPPED cars driving themselves on automated highways. A scene out of "The Jetsons?" Not exactly. Smart cars and highways have quietly emerged as the latest and most expensive proposal to solve the nation's traffic problems. Government spending on the little-known Intelligent Vehicle and Highway Systems (IVHS) program is expected to exceed \$40 billion over the next 20 years. (By comparison, in the first 10 years of the Strategic Defense Initiative, Washington spent \$30 billion.) Even more astonishing is the total lack of organized opposition to the idea, despite evidence that smart cars and highways may well exacerbate the very problems they are supposed to solve.

IVHS would put computers in charge of everything from timing the traffic signals to deciding which route each car should take - and, eventually, to doing the actual driving. In the early stages, a dashboard screen would display maps while a synthesized voice would purr directions to the driver. Later would come the crowning glory of IVHS, the Automated Highway System. Once commuters keyed in their destination, they could just sit back and enjoy the ride - maybe even take a nap. Cars would hurtle along, bumper to bumper, at speeds measured in miles per minute.

The article continues with the following key points:

- o \$218 million of federal funding in 1993
- o claims of improved safety are unproven
- o central computer failures could lead to massive accidents
- o proponents concerned with limiting liability for failures
- o proposed fuel savings from smoother driving could be lost through higher speeds
- o main proponent of scheme is IVHS America, supported by 500 organizations including IBM, AT&T, Rockwell, General Motors, Chrysler, Ford
- o minor attention given to smart public transport, priorities for high-occupancy vehicles

Participants in RISKS will shudder at the thought of testing computer programs design to control thousands of cars in lockstep at 200 kph. I wouldn't enjoy being part of the beta-test population. I wonder how much attention will be paid to deliberate or accidental interference?

- o Presumably information will be transmitted through radio-frequency modems. What will the unique identifiers be for each car. What happens if two cars have the same identifier?
- o How will partial or total breakdown of the control systems be handled? Car-to-car signalling?

o What methods will be put into place to prevent spurious instructions from being accepted by car controllers?

I find the concern with legal liability an alarming indication of where we're headed.

Good fun for those interested in reliability and security; not so good fun for early users, I fear.

Michel E. Kabay, Ph.D. Director of Education National Computer Security Assn

Risky Demo Offer

Rex Wheeler <0003658705@mcimail.com> Thu, 16 Dec 93 13:10 EST

I received an interesting thing in the mail yesterday. It was an unsolicited advertisement/demo for a mail system to run on a Novel PC LAN. It came with a disk that included the instructions: 1) Log into your server as SUPERVISOR, 2) Create a directory for the mail software (In SYS:PUBLIC), 3) copy the contents of the floppy to the new directory, and 4) Run the install program.

There is also a postcard that you can send in to receive a free t-shirt. All you have to do is provide your Name, Title, Company, Address, Telephone, Fax, Signature, and your "unique code number" (which presumably the software will provide you.)

To sweeten the offer there is another card you can send in to enter to win a Jeep and other prizes. This card asks for similar information.

If you run the demo and follow the instructions, you will have executed unknown software from a fully privileged account, and told this company where to find you and your computers.

Sounds like an great opportunity for a Trojan Horse. The "unique code number" could also easily contain information that indicates what else is on your system that may be of interest to this company.

Rex Wheeler rwheeler@mcimail.com (365-8705) 70712.110@compuserve.com

"Re-Chipping" Stolen Mobile Phones

<Brian.Randell@newcastle.ac.uk>
Wed, 15 Dec 1993 11:52:29 GMT

[Following is the complete text of an article in the 15 Dec 1993 edition of the (UK)Independent. I am somewhat surprised at the claimed extent of "re-chipping" of stolen mobile phones, and at the fact of it being legal, but have no basis on which to dispute the facts as stated. Brian Randell, Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne, NE1 7RU,

UK Brian.Randell@newcastle.ac.uk +44 91 222 7923]

LOOPHOLE ON STOLEN PHONES ATTACKED, Patricia Wynn Davies, Political Correspondent

BRITAIN'S latest crime wave - the reprogramming of hundreds of thousands of stolen mobile telephones - is legal, while the necessary technology is openly advertised in newspapers and magazines. Telephones automatically barred from networks when a theft is reported are re-entering the system in their thousands after being "rechipped" by people the law does not treat as criminals.

Robert Maclennan, the Liberal Democrat home affairs spokesman, has written to Michael Howard, the Home Secretary, urging the closure of the legal loophole. Organised rings of mobile phone thieves were getting "easy pickings" amounting to about 350M pounds a year, Mr Maclellan said.

The rechipping process, involving the reprogramming of serial numbers so that the network no longer recognises the phone as the stolen original, can be easily accomplished using equipment that can be plugged into an ordinary home computer.

Chipping services offered by dealers and openly advertised in trade magazines and newspapers have been defended as a necessary facility for honest customers buying second-hand telephones from previous owners who have run up bad debts during the recession. But the biggest beneficiaries appear to be criminals.

The reprogramming racket has provided a ready outlet for small and big-time thieves - the black market price of up to (pounds) 150 for a stolen cellphone easily outstrips that of a stolen car stereo - while spawning a mini-industry of "phone chippers" turning out new sets of chipping software each time a new model is launched.

Thefts are estimated by the industry to be running at 10,000 a month, more than 400 each day, while police forces around the country believe they account for 40 per cent of city-centre car break-ins.

Mr Maclennan has told Mr Howard that the loophole could be easily closed with a minor amendment to the 1984 Telecommunications Act in the forthcoming Criminal Justice Bill.

"This is straightforward counterfeit, but astonishingly it is not illegal," he said. "The police know who many of the crooks are, but cannot touch them."

A similar process of "cloning" a subscribers' serial and telephone numbers into another person's phone results in innocent subscribers being billed for fraudulent calls. Both processes render the phone untraceable.

Interactive TV: electronic democracy, risks to privacy, etc.

John Gray <grayjw@cs.aston.ac.uk> Thu, 16 Dec 93 14:02:33 GMT On UK television last night, a regular evening programme, "The Late Show" was concerned with forthcoming developments in television. This centred around the potential for high bandwidth and bidirectional communications offered by the use of optical fibre for cable TV services.

This increase in the number of channels, some with an interactive content (shopping channels, databases, computer games) would promote the concept of configurable TV ("MeTV" was the name they chose) which allows the user to decide what kind of things they wish to watch, and thus they will largely use only one channel: the one they have configured.

Interestingly, one of the contributors raised the privacy issues: if you know exactly what TV programmes someone likes watching, then you (or your computer system) can tailor direct mail (and even TV adverts) to have the maximum impact. The difference between this and standard audience research is that the *viewer* builds a profile for the advertiser, when they configure the system.

Also in the programme, an executive for CBS raised the point that if everyone only subscribes to compilation services, where does the original material come from? If people select what they view in advance, will they miss out on things that might entertain and enlighten them. The suggestion was made that people will retreat much more into their own pursuits and that "community" will suffer. What happens to people who are too poor to have cable, either because their neighbourhood isn't cabled, or because they can't afford to subscribe. They also touched on electronic democracy in this context: if you can't afford to subscribe, will you have a voice on an equal footing with others?

Finally, a contributor from the EFF suggested that the Internet be used as a model: the idea of providing these services to form communities controlled by users rather than by large companies or governments. Sadly, it seems as if the commercial attractions to advertisers and corporations will win out.

John Gray

Trouble with funny place names

Mark Brader <msb@sq.com> Fri, 17 Dec 1993 22:50:00 -0500

In the Usenet newsgroup rec.puzzles, there has been a little discussion recently of place names with unusual characters. It was suggested that Westward Ho!, England, was unique for containing the punctuation mark "!", but then somebody topped this by calling attention to Saint-Louis-du-Ha! Ha!, Quebec, Canada.

At this point I decided to look these places up in atlases to see where exactly they are. The one I found Saint-Louis-du-Ha! Ha! in was the Rand McNally Road Atlas, 1991 edition.

In the index, the place is spelled... "St.-Louis-du-Ha90 Ha90".

Mark Brader Toronto utzoo!sq!msb msb@sq.com

(P.S.: Westward Ho! is on the north coast of Devon, more or less straight north of Plymouth. Saint-Louis-du-Ha! Ha! is about halfway between Riviere-du-Loup, Quebec, and Edmundston, New Brunswick.)

Mexico Turns Off Quake Warning System

F E Carey +1 908 949 8049 <fec@arch4.ho.att.com> Sun, 19 Dec 93 15:21:52 EST

Mexico's earthquake warning system has been turned off after failing at least twice since it went into operation in August. In October a quake measuring 6.8 on the Richter scale hit but the alarm didn't sound. In November a false alarm went out on a calm Tuesday evening. Technologically, the system is fairly simple. Solar powered seismic detectors signal a desktop Olivetti. Radio stations receive signal directly from the Olivetti system and broadcast warbling tones like something from a science fiction movie. Professor of Engineering Juan Manuel Espinosa Aranda, head of the warning system, said it was tested for two years before going into operation. He said the two failures resulted from simple, though lamentable, errors adding that it is better to have a warning - even if it might be false - than simply to let nature take its course. Not all share his view. Cinna Lomnitz, a seismology professor, said: "Basically, this is an experimental system that should not be broadcast to the public right off the bat. Indirectly, these people have damaged our reputation as seismologists." Luis Abraham Villa, an office assistant, said: "It creates collective hysteria. It really affects the older people. They go crazy."

Reported in The New York Times, 12/19/93

Frank Carey at Bell Labs f.e.carey@att.com

Wireless Laptop Eavesdropping

Andrew Duane USG/PE <duane@zk3.dec.com> Mon, 20 Dec 93 15:47:00 EST

I just saw a blurb on "The Computer Chronicles" about the last Comdex show, which focussed on portables, laptops, notebooks, and accessories for them. One new product, whose name I didn't catch ("AirLink"?) was a wireless device that automatically downloads all of your modified files as soon as you get within 30 meters of your PC. There is no user interface at all. It even works through walls.

The possibilities for data theft are endless. Apparently, there is not even a warning that downloading is occurring. It seems that once these are common, an industrial spy could wander O'Hare airport and download a lot of files if he/she were so inclined.

Does anyone have more information on this product?

Andrew L. Duane, Digital Equipment Corporation USG Kernel Scalability Nashua, NH 03062-2698 603-881-1294 duane@zk3.dec.com

★ Re: Harry Erwin on Digital Woes (RISKS-15.34)

Lauren Wiener <lauren@reed.edu> Thu, 16 Dec 93 17:38:23 -0800

I was certainly interested to read Mr. Erwin's contribution. "Digital Woes" is intended to highlight a widespread problem to an audience that is essentially oblivious to such matters (certainly not the RISKS audience!). While the problem of unreliable and overly costly software is undeniably widespread, it would be simple-minded to insist that it is universal. Categories are ordinarily fuzzy; exceptions make life interesting, after all. (I myself am having the pleasure, at present, of working for folks who write specs!)

It is entirely possible that the project Mr. Erwin describes is such an exception. If so, let me add my congratulations to Mr. Distaso's. However, I am curious to learn more about this project -- especially if it *was* exceptional. In particular, I am curious to learn:

- * What was the purpose of the software?
- * What was it supposed to do?
- * Was the product actually used in real-world situations, as opposed to testing?
- * Were the acceptance tests specified in advance? Were they available to the developers to use as they developed the software?
- * If the product was used beyond testing, did it satisfy the real-world requirements as well as the tests?
- * If the project was a contract with the U. S. gov't, was it in the interests of both the subcontractor and the government to declare the project a success? Did this equate to a big career win for all the parties involved? (Unfortunately, the incentives are often such that it is in the interests of neither party to point out weaknesses in the product. This kind of arrangement can make such congratulatory letters sound a bit hollow.)

It is entirely possible, of course, that the project Mr. Erwin describes had none of these weaknesses, and was in fact a true and marvelous success. All the more reason to learn more about it, if possible. It would be wonderful to isolate even one factor that could help the rest of us.

✓ Question About Singapore Lottery Crime

Sanford Sherizen <0003965782@mcimail.com> Mon, 20 Dec 93 19:03 EST

I am trying to find some detailed information about a recent case in Singapore where a systems person who worked for the national lottery was able to fix or determine in advance the winning number and tip off a friend who placed a bet. The individuals were recently found guilty and sentenced. If anyone knows the details, please post on RISKS or send to me. Thanks.

Sanford Sherizen Data Security Systems Natick, Massachusetts

ISOC Symposium on Network and Distributed System Security

Dan Nessett <nessett@ocfmail.ocf.llnl.gov> Mon, 20 Dec 1993 11:29:21 -0800

Wednesday, February 2

6:00 P.M. - 8:00 P.M.

Registration and Reception

Thursday, February 3

7:30 A.M.

Continental Breakfast

8:30 A.M.

Opening Remarks

9:00 A.M.

Session 1: Electronic Mail Security

Chair: Steve Kent (BBN)

Certified Electronic Mail, Alireza Bahreman (Bellcore) and Doug Tygar (Carnegie Mellon University), USA

(Carriegie Mellon Oniversity), OSA

Privacy Enhanced Mail Modules for ELM, Selwyn Russell and Peter

Craig, Queensland University of Technology, Australia

Management of PEM Public Key Certificates Using X.500 Directory

Service: Some Problems and Solutions, Terry Cheung, Lawrence

Livermore National Laboratory, USA

11:00 A.M.

Session 2: Panel: Public Key Infrastructure, Santosh Chokhani (MITRE),

Michael Roe (Cambridge University), Richard Ankney (Fischer, Intl.)

Chair: Miles Smid (NIST)

2:00 P.M.

Session 3: Protocols

Chair: Tom Berson (Anagram Labs)

Paving the Road to Network Security, or The Value of Small Cobblestones, H. Orman, S. O'Malley, R. Schroeppel, and D. Schwartz, University of

Arizona, USA

A Complete Secure Transport Service in the Internet, Francisco Jordan and Manuel Medina, Polytechnical University of Catalunya, Spain

3:30 P.M.

Session 4: Internet Firewall Design and Implementation

Chair: Jim Ellis (CERT)

Inter-LAN Security and Trusted Routers, Pal Hoff, Norwegian Telecom Research, Norway

Trusted to Untrusted Network Connectivity: Motorola Authenticated Internet Access -- MANIAC(TM), Bill Wied, Motorola, USA

BAfirewall: A Modern Firewall Design, Ravi Ganesan, Bell Atlantic, USA A Network Perimeter With Secure External Access, Frederick Avolio and Marcus Ranum, Trusted Information Systems, USA

7:00 P.M. Banquet

Friday, February 4

8:30 A.M.

Session 5: Panel: All Along the Watchtower: Experiences and Firefights Managing Internet Firewalls, Bryan Boyle (Exxon Research), Brent Chapman (Great Circle Consulting), Bill Cheswick (AT&T Bell Labs), Allen Leibowitz (Warner-Lambert), Paul Vixie (Vixie Enterprises)

Chair: Marcus Ranum (TIS)

10:30 A.M.

Session 6: Issues in Distributed System Security

Chair: Cliff Neuman (USC-ISI)

CA-Browsing System -- A Supporting Application for Global Security Services, Denis Trcek, Tomas Klobucar, Borka Jerman-Blazic, and Franc Bracun, Jozef Stefan Institute, Slovenia

The X.509 Extended File System, Robert Smart, CSIRO Division of Information Technology, Australia

Auditing in Distributed Systems, Shyh-Wei Luan (VDG, Inc.) and Robert Weisz (IBM Canada Laboratory), USA/Canada

1:30 P.M.

Session 7: Authentication

Chair: Dave Balenson (TIS)

The S/KEY(tm) One-Time Password System, Neil Haller, Bellcore, USA A Technique for Remote Authentication, William Wulf, Alec Yasinsac, Katie Oliver, and Ramesh Peri, University of Virginia, USA Remote Kerberos Authentication for Distributed File Systems: As Applied to a DCE DFS-to-NFS File System Translator, Thomas Mistretta and William Sommerfeld, Hewlett-Packard, USA 3:30 P.M.

Session 8: Panel: IP Security Alternatives, K. Robert Glenn (NIST), Paul Lambert (Motorola), David Solo (BBN), James Zmuda (Hughes)

Chair: Russell Housley (Xerox)

PROGRAM CO-CHAIRS

Russell Housley, Xerox Special Information Systems Robert Shirey, The MITRE Corporation

GENERAL CHAIR

Dan Nessett, Lawrence Livermore National Laboratory

PROGRAM COMMITTEE

Dave Balenson, Trusted Information Systems

Tom Berson, Anagram Laboratories

Matt Bishop, University of California, Davis

Ed Cain, U.S. Defense Information Systems Agency

Jim Ellis, CERT Coordination Center

Steve Kent, Bolt, Beranek and Newman

John Linn, OpenVision Technologies

Clifford Neuman, Information Sciences Institute

Michael Roe, Cambridge University

Robert Rosenthal, U.S. National Institute of Standards and Technology

Ravi Sandhu, George Mason University

Jeff Schiller, Massachusetts Institute of Technology

Peter Yee, U.S. National Aeronautics and Space Administration

BEAUTIFUL SAN DIEGO

The Symposium venue is the Catamaran Resort Hotel, providing 7 acres of gorgeous surroundings, facing Mission Bay and only 100 yards from beautiful Pacific Ocean beaches. Spouses and family members can catch a convenient Harbor Hopper for a quick trip to Sea World. After the Symposium, plan to spend the weekend visiting La Jolla, the world famous San Diego Zoo or Mexico, only 30 minutes by car or Trolley.

A limited number of rooms have been reserved at the Catamaran for the very special rate of \$77 single, \$87 double. Reservations, on a space available basis, can be made by calling (800) 288-0770 and indicating you are attending the ISOC Symposium. Reservations must be made before Jan. 1, 1994 to ensure this rate.

CLIMATE

February weather in San Diego is normally very pleasant. Early morning temperatures average 51 degrees while afternoon temperatures average 67 degrees. Generally, a light jacket or sweater is adequate during February; although, occasionally it rains.

TRANSPORTATION

San Diego International Airport is 10 miles (15 minutes) from the Catamaran Hotel. Supershuttle operates a continuous service between the airport and the hotel: fare is \$6.00. When you arrive at the airport, use the free Supershuttle phone. Taxi fare between the airport and the hotel is \$20. The Catamaran charges \$6 per day for parking.

REGISTRATION FEES

Postmarked Subsequent by Jan. 1 registration

\$305 \$350

No refunds after Jan. 20.

REGISTRATION INCLUDES

- Attendance - Symposium Proceedings

- Reception - Banquet

- Luncheons - Coffee Breaks

On-site registration is available Wednesday evening at the reception, and Thursday morning at the Symposium. For more information on registration and local arrangements contact Dan Nessett at (510) 422-4033 or nessett@llnl.gov.

SYMPOSIUM REGISTRATION FORM

Name
Affiliation
Name on Badge
Vegetarian Meals?
Mailing Address
(Area Code)Phone #

Make check (credit cards not accepted) payable to SNDSS94. (Registration is not effective until payment is received). Mail to: ISOC Symposium, C/O Belinda Gish, L-68, Lawrence Livermore National Laboratory, Livermore, CA. 94550.



Email Address _____

Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 36

Sunday 2 January 1994

Contents

Risks of high pitched tones

Lance J. Hoffman

Can SETI signals bear viruses?

Brandon A Cantillo

Report on Strasbourg A320 Crash emphasises HCI

Peter B Ladkin

Be careful not to let your engine control computers overheat.

Peter B Ladkin

LapLink Wireless

Mark Eppley via Bob Frankston

Re: Airport lessons for InfoSec

Robert Dorsett

Re: "Re-Chipping" Stolen Mobile Phones

Andrew Beattie

Li Gong

An Exception

Harry Erwin

Info on RISKS (comp.risks)

risks of high pitched tones

"Lance J. Hoffman" <hoffman@seas.gwu.edu> Sun, 26 Dec 1993 10:07:07 -0500 (EST)

>From the Washington Post, Dec. 26, 1993: >From "1993: The year of the weird" (page C3)

The Syracuse Herald-Journal reported in January that its telephone hotline, featuring excerpts of the presidential debates last fall, was succeesful except for one glitch: Ross Perot's voice sometimes hit a pitch that mimicked a certain telephone tone that automatically shut down the whole system.

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

Can SETI signals bear viruses?

Brandon A Cantillo <cantillo@world.std.com> Sun, 26 Dec 1993 05:15:41 GMT

I wonder if there are any protocols in place or even proposed for "quarantining" signals detected by SETI programs against the possibility of viral infections in software? If Turing machines are a universal feature of mathematics, might not a malicious or possibly just careless civilization be transmitting open or disguised programs that could conceivably wreak havoc among our delicate infosystems? Has anyone thought of this possibility and its implications? Or has this subject been done to death already and I've missed it? If so any pointers to the info at any archive site gratefully appreciated. If not, surely it merits some serious discussion? After all, we were so afraid of biological contamination the first few Apollo crews were in isolation for days until we determined that there was no danger. We should have the same concern for informational "contamination" today, since so much of our civilization depends on Turing machines.....

["Just careless" would seem unlikely if they were an advanced civilization. There is always a possibility that an unanticipated signal might do something strange to a system. There are lots of cases of electromagnetic interference in the RISKS archives, for example. But if everything in SETI is interpreted properly as pure DATA, you don't need to worry. BTW, if we had tapes long enough for the Turing machines, they might be able to reach to distant planets. PGN]

★ Report on Strasbourg A320 Crash emphasises HCI

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
22 Dec 93 21:10:28 GMT (Wed)

Flight International, 22/12/93-4/1/94 p11 contains an article on the report of the commission of inquiry into the Jan 1992 Strasbourg A320 crash. Details and comments on the preliminary findings have appeared in RISKS before. E.g. see RISKS-14.01 (Mellor) on a rumor of a possible transient fault in the FMGS. The crew set up an unusually high rate of descent (3,300 ft/min) instead of the usual 800 ft/min (the final approach fix is only at 1,500 ft above ground level). FI's report focuses on the crew training and the interface problems highlighted by the report.

"The commission concluded that the crew's "below-average" performance contributed to the accident and that the low combined time on type of the two pilots (162h captain/61h co-pilot) caused a lack of familiarity with the equipment on the A320's flightdeck, which has "...increased the risk factor". [...]

From the moment of descent until impact, says the report, the aircraft's high descent rate was adopted and maintained. The commission observed that the "vertical navigation" was left entirely to the automatic systems and the crew appeared to ignore all the clues available to them about

their abnormally high descent rate.

The commission says that the reason for the crew's descent mode selection is not proved beyond all doubt, but that the most probable explanations are a confusion as to which descent mode - vertical-speed (VS) or flight-path-angle (FPA) - was set, having either forgotten to set it or having set it incorrectly.

The ergonomic design of the descent-more selector is criticised for being too easy to misread or mis-set. Airbus states that a design improvement [..] has already been certificated and incorporated into all new A320s since November 1993. A retrofit package will be available for fitting from January 1994.

The many recommendations in the report concentrate heavily on the need for regulation to ensure pilot training and procedures improvements, together with a need to monitor and standardise symbology development in modern flightdeck displays."

Peter Ladkin

✓ Be careful not to let your engine control computers overheat.

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 22 Dec 93 21:20:52 GMT (Wed)

Flight International, 22/12/93-4/1/94, p11.

"Dangerous overheating in an Airbus Industrie A320 engine-starter unit led to complete in-flight engine-control failure [..].

The starboard [engine] suddenly wound down to idle power at 4,000ft (1,200m) in the climb from London Heathrow on 13 December, 1992.

Reversion to manual control had no effect because the circuit breakers for the full-authority digital engine control (FADEC) and engine-interface until had tripped and would not reset. The aircraft returned safely to Heathrow. [...] Temperatures reached 400\degC inside the engine cowl, damaging the FADEC wiring. The AAIB says that the engine wind-down was probably caused by short-circuiting, which gave false signals about thrust-reverser position.

In October 1989 a similar [..] event led to the issue of the 1991 Service Bulletin. A Bulletin issued after the incident was not applied to the [aircraft in this report]. The AAIB recommends making it mandatory."

Peter Ladkin

LapLink Wireless

<Bob_Frankston@frankston.com> Thu, 23 Dec 1993 02:36 -0400

To: Bob Frankston "Robert M. Frankston / MCI ID: 100-7411"

From: Mark Eppley / MCI ID: 296-7039 @ mci

Date: 12-23-93 01:55:00 EST (12-23-93 02:19:57 EST)

Subject: RE: From Risks Digest

It is called LapLink Wireless. Uses FM phase lock loop radio transceivers we developed and licensed to National Semiconductor. He is way off base. 2 levels of security exist as well as compression/encryption of packets flying through the air.

★ Re: Airport lessons for InfoSec (Kabay, RISKS-15.35)

Robert Dorsett <rdd@cactus.org> Wed, 22 Dec 93 21:58:55 CST

Of course, another take on this situation (and equally applicable to the computer world) is that the security culture mainly benefits its vendors and overseeing bureaucracy: that the slipshod techniques are merely there to reassure a naive public that the airlines and their government are doing something with respect to an issue that gravely concerns many: but evidence had repeatedly shown--even at the peak of "red scares"--that these measures tend not to deter the high-risk attackers (or even catch very many of the low-risk attackers, as the estimated ~30,000 security violations/year testifies). EVEN when conducted according to specification.

Metal detectors are manned by poorly trained, low-cost personnel, and provide a single point of entry that is easily subverted. Similarly, badges are ineffective, and door combination locks are easily compromised. But they do show the public that "something is being done." So when hijackings to Cuba became embarrassing, checkpoints appeared; when bombings occur, the call for outrageously expensive explosives detectors goes up; when an airline employee kills the flight crew of an airplane, the employees are treated like criminals (every airline pilot in the United States must pass through the same security checkpoints as the passengers, for instance: in Russia, they ARM their pilots :-)).

This is all visible to the public, and may provide (as with computer security) some level of deterrence for *honest* individuals, but overall, the results are mixed, at best. Countries that do security right (such as Israel) do it very slowly, and very expensively; countries that want their cake and be able to eat it too (profitable security; the closest analog may be network security), resort to symbolic measures, largely ineffective--but which help sell a notion that "something is being done."

So, as with computer security, perhaps the real question to ask is whether the symbolism--for all its faults--is really worth it. I don't particularly relish the prospects of living in a police state, myself. Actually, I *did* live in one, for over ten years. Sure, you can go to sleep with the front door wide open, but such societies take their toll in much more profound, disturbing ways than petty violence.

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

✓ Re: "Re-Chipping" Stolen Mobile Phones

Andrew Beattie <andrew@tug.com> Thu, 23 Dec 1993 10:22:35 +0100

I have had a keen interest in this problem since my portable was stolen from my car. This is what I have since learnt:

Re-Chipping is a misnomer. All modern cellphones can have *soft* Electronic Serial Numbers (ESNs) and phone numbers. On my NEC P3, these can be changed without even removing the cover.

The real thief is the airtime company. They leave me with two choices:

- 1) Pay UKP137.00 to get out of my airtime contract. (3 months line rental, plus UKP50.00 disconnection +tax)
- 2) Buy a new phone. They have a whole department to sell theft-replacement phones. The prices for phones sold without a new airtime contract are *much* higher than those sold with a contract.

The reality is that people generally only upgrade their phones when they get stolen, so it is in the interest of the airtime providers to sell phones with a high "black" value.

The entire trade in stolen phones could be stopped by the simple expedient of using *hard* ESNs and dipping the circuitry in epoxy.

Andrew

★ Re: "Re-Chipping" Stolen Mobile Phones (Brian Randell)

Li Gong <gong@csl.sri.com> Wed, 22 Dec 93 14:02:20 -0800

The rechipping is a service provided even by the Taiwan government, at about NT\$4000 (about US\$160) a pop. Lots of people who are legally registered and paying customers buy cell phones from the US and rechip them to use in Taiwan. The reason is quite legitimate -- the cost of buying a cell phone in Taiwan is exceedingly high. Presumably, by providing this service, the Taiwan government gets fees that would have gone into phone dealers' pockets.

Li Gong, SRI International

An Exception

Harry Erwin <erwin@trwacs.fp.trw.com>
23 Dec 1993 00:35:33 GMT

I was a little surprised my comment got posted, since I was basically interested in the moderator's opinion on why software typically had so many problems. BMDSTP project was unusual in being successful, and I was looking

for some comparably successful projects. Lauren Wiener asks some sharp questions:

1. What was the purpose of the software?

This was the Site Defense Program, which was to build software for the ballistic missile defense system that followed Safeguard. It was also the testbed for Modern Programming Practices, and Barry Boehm was involved. ALTHOUGH the management was good, it was not particularly better than management I've worked with since. The BMDSTP managers did take a proactive stance, trying not to be blindsided by problems, and they were always willing to listen to their engineers.

This program was redirected in midstream in response to the ABM pact, and instead went to Kwajalein as a tracking and data collection tool for the phased array radar out there. It ran on a pair of CYBER 7000 machines. It worked, and it worked well.

2. Was the product actually used in real-world situations, as opposed to testing?

Hard to answer. It ended up a component of a test system, but it was not under test there. It certainly met its requirements.

3. Were the acceptance tests specified in advance? Were they available to the developers to use as they developed the software?

Yes, we were very careful to get the required performance envelope and functional requirements defined in detail, and we ran off-nominal stress tests against those requirements. The real-time operating system was specified top-down, with performance requirements as well as functional requirements, and we built an automatic testing system that validated the RTOS and DMS for each delivery. I've not seen anything since like the way that process was managed. Most programs address performance and reliability late, if ever, and we addressed it from the beginning. As Tom Bell puts it: "Pay me now or pay me later. It'll cost more later." We paid up front.

I'm very interested in why this one program worked so well. I've been observing the FAA Advanced Automation Program for the last three years and trying to understand the difference between my experience on the BMDSTP and their current experience. My impression is that there is a non-linear relationship between the effectiveness of technical management and the success or failure of a software project. If the software is just slightly too hard for the management team, they fall behind and spend their time playing catch-up and responding to surprises. If they are able to get their arms around the system early, on the other hand, they can keep ahead of the problems and control things much more effectively. There's not that much of a difference between most managers and engineers that I can identify, so I suspect it's the nature of the software development problem to be like that.

Does that help?

Harry Erwin Internet: herwin@cs.gmu.edu or erwin@trwacs.fp.trw.com

[Yes, Thanks. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 37

Monday 3 January 1994

Contents

Hacker nurse makes unauthorised changes to prescriptions

John Jones

Customs Data Diddling

Mich Kabay

Credit cards again

Mich Kabay

Tax Frauds

Mich Kabay

Re: Can SETI signals bear viruses?

Robert Ayers

Dave Weingart

James Abendschan

"When H.A.R.L.I.E. Was One" by Gerrold

Rob Slade

Request for help with RISKy situation

Alan Wexelblat

Info on RISKS (comp.risks)

Hacker nurse makes unauthorised changes to prescriptions

John Jones < J.G. Jones@computer-science.hull.ac.uk> Mon, 3 Jan 94 10:09:41 GMT

The Guardian (21st December, 1993) reports the conviction of a male nurse who hacked into a hospital's computer system and modified entries, including prescriptions. The hacker:

- prescribed drugs normally used to treat heart disease and high blood pressure to a 9 year old with meningitis. This change was spotted by a ward sister;
- prescribed antibiotics to a patient in a geriatric ward. These drugs were administered to the patient, with no apparent adverse reaction;

- "scheduled" an unnecessary X-ray for a patient;
- "recommended" a discharge for another patient.

The hacker gained access to the computer system after learning the password through observing a locum doctor having trouble logging in.

He qualified as a nurse in 1989. He is reported to have undergone a considerable personality change as the result of a road accident in 1984. As well as developing a fascination for computers and other hi-tec equipment, he had apparently developed a "lack of sensitivity to the consequences of his actions".

He had been sacked for unprofessional behaviour in 1990, but was re-employed in 1992 at the same hospital.

He pleaded guilty to unauthorised modification of computer records. He offered no explanation for his actions, but denied any malicious intent. He was jailed for 12 months.

John Jones (jgj@dcs.hull.ac.uk)

Customs Data Diddling

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 02 Jan 94 21:12:25 EST

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

Customs-Whistleblower, By Michael White, Associated Press Writer SAN DIEGO (AP, 30 Dec 1993) -- Some of what Mike Horner regards as his best work ultimately destroyed his career as a U.S. Customs Service inspector on the Mexican border. Horner left the service after alleging that intelligence reports he filed identifying suspected drug smugglers and their vehicles were deleted from Customs' computer network."

This article and another by the same author detail the apparent data diddling that resulted in first deleting, then re-introducing, Mr Horner's records of smuggling across the US/Mexican border.

Horner's allegations of malfeasance were ignored by his superiors.

No one can explain how his deleted entries could have re-appeared after he left the U.S. Customers Service.

White's next story is

Customs Smuggling, By Michael White, Associated Press Writer LOS ANGELES (AP, 30 Dec 1993) -- Weaknesses in U.S. Customs' cargo tracking system may have opened a door for smugglers of drugs and other contraband

and cost taxpayers millions of tariff dollars, according to sources and Customs records.

Among the problems: False inspectors' names are showing up on cargo entry records, passing containers without inspection; and seals placed on containers bound for distant destinations are breached in transit, allowing contraband to be removed or contents stolen between the dock and inspection points."

This article deals with irregularities in the computer system used to monitor the Port of Los Angeles.

Key points of the article:

- o some bonded cargos appear to be opened illegally, allowing contraband to be removed.
- o some inspection records online include names of nonexistent officials;
- o records of suspicious shipments which should have initiated followups have been overridden with false names.
- o 200-400 records of in-bond cargo containers are purged each month because the Customs Service cannot trace the containers; an indendent study by the Treasury Department estimated data destruction in the thousands per month.
- o Some employees say that the computer system fools inspectors into relying on electronic records instead of their own initiatives when deciding which shipments to inspect.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Credit cards again

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 02 Jan 94 21:11:50 EST

>From the Reuter newswire via Executive News Service (GO ENS) on CompuServe:

Britons Charged with Europe-Wide Credit Card Fraud

LONDON (Reuter, 30 Dec 1993) - Three Britons have been charged with conspiracy in a 2.5 million pound (\$3.7 million) Europe-wide credit card fraud, police said on Thursday."

The article says that the Birmingham men are accused of having used fake credit cards and stole expensive products in France, Britain, Belgium and the Netherlands. Apparently other arrests are promised.

Once again we see that one of the world's most frequently used network access control tokens, the common credit card, is wholly inadequate to protect the public and the banking industry against fraud.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Tax Frauds

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 02 Jan 94 17:40:16 EST

>From the Washington Post newswire via Executive News Service (GO ENS) on CompuServe

IRS Charges Tax Preparer With \$1.1 Million Fraud, By Christopher B. Daly Special to The Washington Post

BOSTON, Dec. 16 - The president of a nationwide tax-preparation service was indicted today on charges that he used computers to cheat the Internal Revenue Service out of more than \$1 million in one of the biggest electronic tax fraud cases on record, officials said.

Richard M. Hersch, 56, of Ardmore, Pa., was accused of using his company, Quik Tax Dollars Inc. of Bryn Mawr, Pa., to file 431 false tax claims and launder \$1.1 million..."

The article provides details of the case. Key points:

- o 12 million returns were filed electronically in the 1992 tax year.
- o Hersch is accused of making up "145 false tax returns using fictitious names and Social Security numbers."
- o He then allegedly used an intermediary company, Drake Enterprises, which is not accused of wrong-doing, to forward the tax returns to the IRS.
- o Hersch received cheques from a local bank which assumed that the bogus returns were OK, based preliminary info from the IRS which simply certified that there were no obvious errors. Since there were no real filers, Hersch appears to have kept all the money himself.
- o Incidentally, Hersch has been indicted in Philadelphia on charges of stealing \$262,865 from Provident Bank by passing bad cheques. He has also been indicted on charges of using other people's AmEx cards for more than \$1000 in unauthorized purchases.
- o Mr Hersch is currently under house arrest.

Comment: how did this man get to run a tax-preparation service at all? Aren't there any background checks for people in this kind of position? And how about some kind of verification of the fake Social Security Numbers? Is it not possible to check that the SSN is assigned to the person for whom the fake return was made?

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

Robert Ayers <ayers@mv.us.adobe.com> Mon, 3 Jan 94 09:17:33 PST

The sci-fi classic "A is for Andromeda" by Fred Hoyle is the story of a SETI signal which is exactly the plans for, and a program for, a very large computer. The excitement begins, of course, when (against the advice of one scientist) the computer is built ...

✓ Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

the person your mother warned you about <phydeaux@med.cornell.edu> Mon, 3 Jan 1994 09:12:52 -0500

Not sure if this has been treated seriously by industry or academia, but in Vernor Vinge's (marvelous and Hugo-winning) _A_Fire_Upon_The_Deep_, this very method was used by a malicious intelligence to take over remote systems. (In the book, one main method of communication is by a cosic equivalent of Usenet (called either the Known Net or (frequently, and accurately) the Net of a Million Lies). The Blight (abovementioned intelligence) transmitted intelligent packets to take over the remote system).

Personally, I don't think that this is going to be much of a problem right now. In order for the information to wreak any real damage (unless you overload the front end with a powerful signal), the viril would need to run, and unless the evil LGMs at the other end somehow know the architecture of the system doing the decoding, I can't see that this is a serious problem.

73 de Dave Weingart KB2CWF phydeaux@cumc.cornell.edu (212) 746-3638

Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

James Abendschan <unkadath!shamus@naucse.cse.nau.edu> Sun, 2 Jan 1994 21:04:28 +0000 (GMT)

I can't help but think you've been reading "Snow Crash" :-)

The relevance is that, in the course of the narrative, it is discovered the antagonist can cause a biological "crash" of the minds of programmers who have "firmwired the binary code in the deep structures of their brain." He picked this data stream from stellar emissions recorded via a SETI-like antenna network.

A bit esoteric, but it made an amusing read.

(The antagonist also vaguely reminded me of H. Ross Perot; odd.)

For those of you interested, the author is Neal Stephenson and the publisher is Bantam Spectra.

James

"When H.A.R.L.I.E. Was One" by Gerrold

"Rob Slade, Ed. DECrypt & ComNet, VARUG rep" <roberts@decus.arc.ab.ca> 30 Dec 93 15:28 -0600

BKHARLIE.RVW 931222

Ballantine Books
101 Fifth Avenue
New York, NY 10003
or
Bantam Doubleday Dell
666 Fifth Avenue
New York, NY 10103
"When H.A.R.L.I.E. Was One", Gerrold, 1972/1988

HARLIE is not a virus. He/it is an experiment in artificial intelligence. For the purposes of the book the experiment is a success and HARLIE is alive: is a person. The plot revolves (slowly) around the efforts of corporate management to kill the project (and HARLIE) and the efforts of the computer (program) and its creators to stave this off. As in most of Gerrold's books, the plot is primarily there to set up dialogues in which he can expound his philosophies. (The most blatant example of this is in "A Rage for Revenge" most of which takes place in a seminar, the largest chunk of which is devoted to an illustration of the standard five-stage model of grieving.)

In both versions, the "virus" is a mere diversion. It has nothing to do with the story at all, and is a discussion point between two characters, never referred to again. Indeed, in the first version it is introduced as a science fiction story, "but the thing had been around a long time before that." Make of this latter statement what you will. My resident science fiction expert can't think of what the prior story might be and ventures that this might be Asimovian self-citation.

Statements have been made that the virus aspect was downplayed in the second version. This is rather ironic. The virus story gets roughly the same amount of ink in both versions, but the early one is definitely superior. HARLIE72 gives a fairly simple and straightforward account of a self-propagating program. In fact, aside from the dependence upon dial-up links, the parallels between the HARLIE72 virus and the actual CHRISTMA infestation fifteen years later are uncanny. Specifics include the use of an information source for valid contacts, and a mutation which loses the self-deletion characteristic.

The HARLIE88 discussion is much more convoluted, bringing in malaria, spores, phages and parasites. The are even two separate invocations of the worm, one lower case and one capitalized, both with different definitions. (One refers to a logic bomb, and the other to a virus directed at a specific target. Neither definition is so used by anyone else.) The end result is a completely iconoclastic set of terminology bearing almost no relation to anything seen in real life.

To further the irony, HARLIE88 could have been viral. HARLIE72 could not: part of the system was advanced hardware which did not exist in other computers. Therefore, while HARLIE72 had the ability to program other computers, such programming could never have resulted in a reproduction without the additional hardware. HARLIE88, however, was software only. To be sure, the environment included "2k channel, multi-gated, soft-lased, hyper-state" processors, roughly a million times more powerful than the home user's "Mac-9000", but still, as one character has it, just chips. HARLIE88 *could* survive, albeit running more slowly, on other computers. However, while one character realizes that HARLIE could be "infectious" the discussion dies out without realizing that the primary tension of the story has just been eliminated.

copyright Robert M. Slade, 1993 BKHARLIE.RVW 931222 Vancouver Institute for Research into User Security Canada V7K 2G6 604-984-4067 ROBERTS@decus.ca Robert Slade@sfu.ca rslade@cue.bc.ca p1@CyberStore.ca

Request for help with RISKy situation

"Alan (Miburi-san) Wexelblat" <wex@media.mit.edu> Thu, 30 Dec 93 15:10:10 -0500

My bank has installed one of those bank-by-phone services. You call up, give your 10-digit account number, password is the last 4 digits of your SSN, and off you go. At the moment the transactions available are purely informational (get balance, get last 5 checks that cleared, etc.), but they say they plan to allow operational transactions (e.g. pay bills, transfer money) soon.

The problems of this kind of system have been well-covered here in the past; what I need help with is also a known problem, but in this case it appears to be particularly severe. To wit:

In this system, if you time out too often or enter incorrect information twice, you are transferred to a human being who is supposed to help you figure out the system. In my case I encountered this human twice. The first time I had misunderstood which subset of the account digits they wanted. When I got to the human, he could apparently see the digits I had typed and he told me the correct digits to use for my account (how helpful, I thought).

I then called back and tried the new digit set, and it still failed twice.

I talked to another human being who revealed that not only did he have on his screen my account #, but also he had the 4-digit password I had typed *and* the correct password. It turns out that there was a data transcription error in my account and they had a wrong SSN for me; thus the password was different than I expected.

The helpful gentleman -- with NO confirmation of who I was -- provided the correct four digits to me!! ARGH! And I wasn't even *trying* to do social engineering.

Now, what I would like help from RISKS readers on is how I should draft my letter of protest/alarm. To whom within the bank/government/BBB/SEC/etc should it be sent? How do I explain to them that (a) they have to guard this information at least as closely as bank-card PINs; (b) they should provide some way for me to change my password; (c) they have to train their people a whole lot better! At the moment I'm tempted to rant and rave at them, but I know a calm, well-thought-out, detailed response is more likely to get the results I want. Should I start off with a phone call? Has anyone on this list dealt successfully with similar problems?

Please send suggestions directly to me; I will summarize back to RISKS and let y'all know if there is any change in the future.

--Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard Media Lab - Advanced Human Interface Group wex@media.mit.edu 617-258-9168



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 38

Saturday 15 January 1994

Contents

\$500k phone fraud

Chuck Weinstock

Wild agents in Telescript?

Phil Agre

"Industry Defies Clinton on Data Encryption"

John Markoff

Encryption Export Control, and Cantwell Bill

Sharon Webb

(Mis)Information spreads like wildfire

Mabry Tyson

Software Management Risks

Harry Erwin

Info on RISKS (comp.risks)

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Tue, 11 Jan 94 16:32:36 EST

A UPI story today says that a Canadian teenager defrauded a cellular phone network out of \$500,000 worth of long distance calls by changing greetings in voice mail boxes so that they would approve calls billed to the Rogers Cantel, Inc. network. Cantel blames Bell Canada's automated long-distance billing service.

Apparently Cantel has started offering customers a service that will keep their cellular phones from accepting third-party calls.

Chuck Weinstock

Wild agents in Telescript?

Phil Agre <pagre@weber.ucsd.edu> Thu, 6 Jan 1994 08:24:00 -0800

The 6 Jan 1994 New York Times carries an article (business section, pages C1 and C4) by John Markoff about General Magic's Telescript language. The article likens software agents to viruses and worms and concentrates on the liability issues associated with a developing "ecology" of bits of software moving around through networks. My first reaction was that the folks at General Magic can't be too happy about the NYT putting this spin on its new product. After all, the problem with viruses and worms is not precisely that they travel but that they multiply, and few applications of agents, at least the ones most commonly envisioned, require unbounded replication. But then I wondered, how safe are we in a world that includes a widely distributed programming language in which a ten-year-old can write a heavy-duty worm? And Risks readers will guffaw at the following sentence in the article's last paragraph: "In an effort to lock the doors against potential vandals, General Magic has designed Telescript so that many of the most common computer security loopholes are impossible". It goes on to mention that General Magic has licensed encryption technology from RSA Data Security. I'm looking forward to the first few reverse-engineered Telescript products.

Best wishes to General Magic.

Phil Agre, UCSD

"INDUSTRY DEFIES CLINTON ON DATA ENCRYPTION" -- John Markoff

"Peter G. Neumann" <neumann@csl.sri.com> Fri, 14 Jan 94 9:38:33 PST

[The following item is copyrighted by the 1994 N.Y. Times, and appeared on Thursday, 13 Jan 1994. It is reproduced in RISKS with the permission of its author. Any further reuse requires permission of the New York Times. PGN]

REDWOOD CITY, Calif. The Clinton administration's newly articulated information technology policy of persuasion, rather than dictation, is getting an early test.

At an industry conference in Redwood City this week, computer hardware, software and telecommunications companies as well as a major bank, are saying they intend to adopt an industry coding standard for protecting the privacy of electronic communications, rather than support a standard being pushed by the administration.

Unlike the administration-backed standard, the technology, which has been commercialized by RSA Data Security Inc., does not provide an electronic "trapdoor" that would enable law-enforcement agencies to eavesdrop on digital communications.

The administration, whose standard is known as the Clipper chip, contends that a trapdoor is necessary to detect criminal activity or espionage because sophisticated encryption techniques can make digital phone calls or computer communications nearly impervious to wiretaps.

Wednesday, Hewlett Packard Co. became the last of the leading United States computer companies to license the RSA software, joining Apple Computer, IBM,

Sun Microsystems, Digital Equipment and Unisys.

Several companies announced at the conference that they planned to begin selling products that embed RSA's software. Among them are General Magic, a software developer; National Semiconductor; a consortium of five cellular data companies, and Bankers Trust Co.

The conference was sponsored by RSA, which is based in Redwood City, and attracted many of the nation's best non-government cryptographers a group of code makers and code breakers who have generally been hostile to any form of government restrictions on their technology.

They have sparred for more than a decade with the National Security Agency, the main proponent of the Clipper chip. The agency is responsible for monitoring electronic communications worldwide for the government, in the name of national security.

In addition to opposition from the cryptographers, the government's Clipper chip proposal has already stirred bitter opposition from civil liberties organizations and computer user groups, who fear the Clipper chip would make electronic communications too easy for anyone to eavesdrop.

Now the industry's rush to embrace an encryption standard that does not provide a way for the government to listen to data or voice conversations is certain to put new pressure on the Clinton administration, which is now in the final stages of a classified review of its Clipper standard.

``It's clear that what is going on here today is contrary to the way the NSA wants the world to move," said Lynn McNulty, associate director for computer security at the National Institute for Standards and Technology, a Commerce Department agency. The institute proposed the Clipper standard last April, although most of its technical development was done by NSA researchers.

Despite their defiance, researchers attending the conference worried that the government might still have the means to enforce its vision of a coding standard.

"They have the trump card that we don't have," said Bruce Schneier, a former government cryptography researcher, who is the author of a textbook titled "Applied Cryptography." "They could make it a law that it's mandatory to use their standard."

National Computer Security Association 1994 Security Summit -

<SHARONWEBB@delphi.com>
Thu, 06 Jan 1994 20:39:24 -0400 (EDT)

Washington D.C. 1-25-94 and Encryption Export Control

[This message was received rather late, even if the R.S.V.P. deadline was extended from 2 Jan! But you may want to respond anyway. Besides, the Cantwell Bill is included below, and it may be of interest to many RISKS readers. PGN]

This is an invitation to join members of the security community, Administration officials, and members of Congress in a discussion of security on the National Information Infrastructure and encryption export controls.

The meeting will be held at the Washington Convention Center on January the 25th, 1994. The meeting will begin at 8 a.m. and will adjourn at 3 p.m.

The purpose of this meeting is in response to a request from Secretary of Commerce Ron Brown at the recent 1993 Technology Summit in San Francisco. Secretary Brown asked that a meeting be held to bring together industry and government to start an open dialog, which will help shape information security policy as the United States moves forward into a more global economy. Everyone will have a chance to express their opinions and concerns.

During this meeting individual committees will be formed to study and make recommendations on specific areas of information security as it relates to the NII (this will also become known as the International Information Infrastructure).

R.S.V.P.'s are required NO LATER THAN January 2, 1994 [apparently extended to 10 Jan. PGN]. Please call Paul Gates at the National Computer Security Association (717) 258-1816. All attendees will be sent an agenda, a copy of the NII, the Clinton Administration's Technology Policy and a copy of the Cantwell Bill which deals with encryption export controls.

NOTE: If you cannot attend in person but would still like to participate we will be offering on-line opportunities.

Sharon Webb voice# (404) 475-8787Director, Legislative Affairs, National Computer Security Association

P.S. Attached please find a copy of the Cantwell Bill, my comments and the NCSA's Encryption Export Control Survey .

Please send ALL responses to either my fax #(404) 740-8050 OR EMAIL to me via SHARONWEBB@ DELPHI.com

103D Congress 1st Session

H.R. 3627

IN THE HOUSE OF REPRESENTATIVES

Ms. CANTWELL (for herself and) introduced the following bill which was
referred to the Committee on	

A BILL

To amend the Export Administration Act of 1979 with respect to the control of computers and related equipment.

Be enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. GENERALLY AVAILABLE SOFTWARE.

Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end thereof the following new subsection

- "(g) COMPUTERS AND RELATED EQUIPMENT -
- "(1) GENERAL RULE. Subject to paragraphs (2) and (3) the Secretary shall have exclusive authority to control exports of all computer hardware, software and technology for information security (including encryption), except that which is specifically designed or modified for -
- "(A) military use, including command, control and intelligence applications; or
 - "(B) Cryptanalytic Functions
- "(2) ITEMS NOT REQUIRING LICENSES No validated license may be required, except pursuant to the Trading With The Enemy Act of the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of-
- "(A) any software, including software with encryption capabilities, that is
- "(i) generally available, as is, and is, and is designed for installation by the user or
- "(ii) in the public domain or publicly available because it is generally accessible to the interested public in any form; or
- "(B)" any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).
- "(3) SOFTWARE WITH ENCRYPTION CAPABILITIES The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end-uses in any country to which exports of such software are permitted for use by financial institutions not controlled in fact by united states persons, unless there is substantial evidence that such software will be -
- "(A) diverted to a military end-use or an end-use supporting international terrorism:
 - "(B) modified for military or terrorist end-use; or
 - "(C) re-exported without requisite United States authorization.
- "(4) DEFINITIONS As used in this subsection-
- "(A) the term 'generally available' means, in the case of software (including software with encryption capabilities), software that is offered for sale, license, or transfer to any person without restriction through any commercial means, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;
- "(B) the term 'as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed,

developed, or tailored by the vendor for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

- "(C) the term 'is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities -
- "(i) the software company intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the company may also provide telephone help line services for software installation, electronic transmission, or basic operations; and-
- "(ii) that the software program is designed for installation by the purchaser without further substantial support by the supplier;
- "(D) the term 'computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process or provide out-put of data; and
- "(E) the term 'computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules and integrated circuits". END of BILL

FROM: Secure Systems Group International, Inc TO: Bob Bales Director, National Computer Security Association (717) 258-1816

Re: Encryption Export Bill (Cantwell) Bob -

Here are some of the comments that we passed along to Maria Cantwell's office regarding the Bill on the export of encryption technologies. I hope you find it useful.

I understood the purpose of this Bill was to reduce export controls and restrictions of software that is either based on encryption or that contained encryption. As I read the Bill everything was fine until paragraph (3) -(You understand that I am reading this from a laypersons point of view and if you can clear up any misinterpretations I would appreciate it).

In paragraph (3) the Bill states software containing encryption can be exported freely "unless there is substantial evidence that such software will be:

- (A) diverted to a military end-use or end-use supporting international terrorism:
- (B) modified for military or terrorist end user or

(C) re-exported without requisite United States Authorization."

or that software which is

- "... specifically designed or modified for
- (A) military use, including command, control, and intelligence applications; or
- (B) cryptanalytic functions

I think that before I or others from the security side decide to support or not to support this Bill we have some questions that need answers.

100 Nobel Court, Suite 400, Alpharetta, GA. 30202 Voice (404) 475-8787 FAX (404) 740-8050

Member of National Computer Security Association and the American Electronics Association

- 1. Who will be asked to determine whether such restrictions are appropriate? The NSA? The CIA? The FBI? Does it remain the same as under the current law? Assuming that the technical overview of military applications for encryption remains the NSA what makes it in their interest to let ANY encryption out of the country that will make their job more difficult? (A little like letting the fox guard the chickens)
- 2. What constitutes substantial evidence 'of or 'designed for' military use? Is it measured by the relative strength of the algorithm or key management system or by the mere fact it is longer than the DES which is 56 bits? I feel that some sort of definition needs to be included. What can and what cannot be exported? A list of commercially available encryption software algorithms that are pre-approved (i.e. DES, RSA, PGP, RC4, DSS, etc.) would be nice. Is selling an encryption product to a foreign military contractor the same as selling to the military itself, and who makes the judgment call?
- 3. Will export licenses be required will denials be explained so that the exporter and the public understand the reasons for the denial?
- 4. If a denial is issued, will the exporter have any forum for appeal?

Since Secretary of Commerce Ron Brown has exclusive control over the export rules, it is obvious that the intelligence community can have a single, important, point of focus for influence. (Yes I an slightly suspicious). In theory, the intelligence overseers could disapprove any license to a FRIENDLY Government or customer on the assumption that their military would use it just because its within their borders. It is unlikely that German forces will revert to DES, but their interest in RSA or PGP or triple DES may have such applications. It would still be in the NSA's best interest to limit the export of such software.

My major objection to the Bill as I have understood it is that Commerce, based

on advice from the intelligence community (i.e. NSA), still has arbitrary control over what encryption may be exported or not. How is this that much different from what we have today?

This version of the Bill would still permit the Secretary to arbitrarily restrict export of some algorithms with no technical benchmarks in place (i.e. length of key, number of bits). There will be some algorithms that the U.S. would want to restrict it would be a great help to all to compile a list of accepted algorithms for export such as is done with computer exports which are measured in MIPS.

In general, I like the Bill - we NEED it ! - but I feel that it leaves a lot of room for confusion.

Let me know what your thoughts are on this - thanks.

Sharon Webb, President
National Computer Security Association Encryption Export Control Survey

The purpose of this survey is to quantify the business opportunities lost because of the U.S. policy on the exportation of encryption algorithms such as DES, RSA, etc. If we are to make ANY impact AT ALL, the security community needs to let Congress that economic HARM is being done due to the export control on encryption technologies.

Please take the time to fill this out and return it to NCSA NO LATER THAN FRIDAY JANUARY 7, 1994. NCSA FAX (717) 243-8642.

The results will be presented to Congress in order to further efforts to release export controls on certain encryption technologies.

- 1) Are you a manufacturer of products that utilize encryption methods?
 - YES NO
- 2) What forms of encryption do you use?
- 3) Is you product Hardware Software or Both.
- 4) Have you experienced a loss of sales OVERSEAS due to export controls?

YES NO

(If the answer is YES, please list the country, the customer (optional), the dollar amount lost and who got the business (Competitor). If there is a way for you to be able to know WHY a bid was lost let us know.)

5) Have you experienced a loss of sales HERE in the U.S. and Canada to foreign competition?

YES NO

(If the answer is YES, please list the customer (Optional), the dollar amount

and who got the business (Competitor).

6) What percentage of your business is U.S. based? International?

(what country(ies) make up the largest portion of your International sales?

Who are you? (Optional) and additional comments: (Use additional paper if necessary)

Attached is a file called NCSASUR.DOC. This file contains an open invitation to the meeting in Washington D.C. on January 25th. Italso contains a copy of the Cantwell Bill and my comments. The final page is the VERY IMPORTANT NCSA Encryption Export Control Survey. We need as many QUALIFIED (names and phone numbers attached) responses ASAP!!!!

Thank You

Sharon Webb - Director, Legislative Affairs NCSA voice#(404) 475-8787 fax# (404) 740-8050 email SHARONWEBB@Delphi.com

✓ (Mis)Information spreads like wildfire

Mabry Tyson <TYSON@ai.sri.com> Sat 8 Jan 94 16:23:27-PST

In the message below, I try to be careful to use "allegedly", "claimed", etc., to indicate information that I have been lead to believe was correct but that I have not checked up on myself. By using these words, I do not mean that the statements are incorrect or correct, only that I am not sure of their veracity.

On Friday, 8-Jan-1994, I received a message (apparently originally sent on Tuesday) that discussed a certain company that was (allegedly) advertising "free Internet access" but required you to Fax them a credit card number. This message was from someone who claimed to be in a position of knowing all the service providers in that area and had checked up on that company. The message indicated that the "Suite" address was just a P.O. Box at a non-US Postal Service provider and the phone number just got you to voice mail. The message also indicated that the Internet address you would get was not registered with the INTERNIC and was not in a couple of (milnet) hosts tables.

I took the message at face-value (I still have no reason to doubt the sender or his intent) and sent a message to another very large and wide-spread mailing list that was a warning about giving your credit card number out to receive Internet access without checking out the company. Thankfully, I chose not to give the name of the company.

A few hours later, David Oppenheimer pointed out in a reply to that same mailing list that the Internet address did in fact exist and was registered to a company of the same name. The addresses were different (different states)

but at this point, I suspect that it is the same company.

I received the original message as a private one from a friend and also saw it distributed on a largish mailing list (to which it had been forwarded from another mailing list).

(On Saturday, I informed the list I saw it on of the corrections that Oppenheimer pointed out.)

I wonder how many people saw the original message that contained some apparently incorrect information. This kind of misinformation can spread so quickly. The corrections may not reach all the people who saw the first message.

(I've just now learned of 8 other mailing lists it was forwarded to.)

There are some lessons to be learned:

- Don't give your credit card number to anyone without checking
 them out
- 2. Don't presume that the info in a message is correct just because someone sent it.
- Don't be too quick to spread information that you haven't checked out personally.
 Misinformation can spread like wildfire. Furthermore, for all I know (not being a lawyer), you might be held legally responsible for spreading it.
- 4. Don't presume that the sender of a message is who he says he is. (NOTE: The sender of the original message may really be who he says he is. However, *I* haven't checked on that.)
- 5. After reading the above, how do you know I am who I say I am?

[I know Mabry and he would never play tricks. He's very reliable. I also checked out the original offer. It was indeed genuine, although somewhat misleading. The Internet connections may have been free, but the users are still going to get stuck for higher-than-usual telephone charges. PGN.]

Mabry Tyson Tyson@AI.SRI.COM

The views and opinions expressed are mine personally and do not necessarily represent the views, opinions, or policies of my employer.

Software Management Risks

Harry Erwin <erwin@trwacs.fp.trw.com> 9 Jan 1994 01:00:57 GMT

Aerospace Daily carried some articles recently that may be able to shed some light on the problems of software development. On 1/6/94, there was an article

on how rigid management appeared to have had a role in the Mars Observer failure. On 1/7/94, there was a similar article on problems with the C-17. The 1/6/94 article was particularly interesting, as it suggested that the failure of the Mars Observer had to do with the use of fuel system parts that had not been qualified for deep space missions. This may have occurred due to management turmoil, leading to the departure of technically-qualified middle management. Without that layer of technical management, the risks of using unqualified parts were not recognized during design reviews. The 1/7/94 article suggests that the C-17 problems were similarly due to a TQM program that eliminated the echelon of technical management that was usually responsible for ensuring a successful system integration.

These two data points are consistent with my experience on the BMDSTP program (discussed in an earlier RISKS). Although, as I indicated, the middle-echelon technical managers on that program were not markedly better than managers I've met since then, they did possess the necessary expertise in their areas to ensure a successful integration of that system. This suggests that the usual management approach to the development of complex computer systems all too often lacks an echelon of technical management necessary to the successful integration of those systems. And it suggests TQM has exacerbated this by eliminating that echelon in some organizations that had previously avoided this problem.

Comments?

Harry Erwin Internet: herwin@cs.gmu.edu or erwin@trwacs.fp.trw.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 39

Friday 21 January 1994

Contents

Hidden risks of earthquakes

Clive D.W. Feather

Phony air traffic controller

Fernando Pereira

Poulson/PacBell

Mich Kabay

Links to Internet to be limited by DoD

Bob Kolacki

India - Software Glitch Causes PSLV Failure

S. Ramani

Verify your backups

Louis Todd Heberlein

Safety in Telescript

Luis Valente

Slippery Folks in the Oil Business

Peter Wayner

Risks of Domain Names

Matt Cohen

Re: Mail forwarding as easy as Call forwarding

John M. Sulak

Cellular phone security features...NOT!

Matthew Goldman

Harvard Case of Stolen Fax Messages

Sanford Sherizen

Re: Hacker nurse makes unauthorised changes to prescriptions

Li Gong

Spontaneous recovery from "NOMAIL" setting?

Ron Ragsdale

Re: Proposal for new newsgroup on safety-critical systems

Jonathan Moffett

Privacy Digests

Peter G. Neumann

ISSA Conference Announcement

Dave Lenef

Info on RISKS (comp.risks)

Hidden risks of earthquakes

"Clive D.W. Feather" <clive@sco.com> Wed, 19 Jan 1994 21:54:21 +0000 (GMT)

Today's (Wednesday) San Jose Mercury News reports a hidden effect of the LA quake this week. The main electric feed to the LA area was knocked out by the quake, darkening the whole basin. However, interdependencies in the grid meant that power supplies went out as far away as Wyoming and Alberta. 150,000 people were without power for three hours in Idaho.

It all goes to show just how interconnected things all are.

Clive D.W. Feather, Santa Cruz Operation, Croxley Centre, Hatters Lane, Watford, WD1 8YN, United Kingdom clive@sco.com Phone: +44 923 816 344

phony air traffic controller

Fernando Pereira <pereira@alta.research.att.com> Thu, 20 Jan 94 16:49:24 -0500

Associated Press writer David Reed reports that an out-of-work janitor pleaded guilty to giving false radio commands to pilots around Roanoke Regional Airport in Virginia. The phony controller, Rodney Eugene Bocook, called the "Roanoke Phantom" by legitimate controllers, would tell pilots to abort landings, change altitudes and direction. Although some pilots followed his instructions, no serious incidents resulted. The phony instructions were sent for six weeks last fall until FAA agents with transmitter-tracking equipment found the source. Bobcook pleaded guilty to giving pilots false information and using profane language over the radio. His attorney claimed that Bobcook was not fully able to understand the gravity of his actions or of distinguishing right and wrong. Under federal sentencing guidelines, it is estimated that he will serve two years.

This raises interesting questions of authentication. Wouldn't it be possible to add to air traffic messages some kind of "signature" that would help receivers distinguish between legitimate and bogus messages?

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave, PO Box 636 Murray Hill, NJ 07974-0636 pereira@research.att.com

[The RISKS archives contain earlier very similar cases. This is by no means a new problem. PGN]

✓ Poulson/PacBell

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> 07 Jan 94 09:45:23 EST >From the United Press Intl newswire via Executive News Service (GO ENS) on CompuServe:

Hacker to ask charges be dropped

SAN JOSE, Calif. (UPI, 04 Jan 1994) -- An attorney for a former Silicon Valley computer expert accused of raiding confidential electronic government files said Tuesday he will ask to have charges dismissed now that a federal judge has thrown out the government's chief evidence.

Attorney Peter Leeming said the government's case against Kevin L. Poulsen is in disarray following a ruling suppressing computer tapes and other evidence seized from a rented storage locker in 1988.'

The article continues with the following key points:

- o Judge ruled that material taken from Poulsen's locker is inadmissable;
- Poulson charged with espionage after alleged hacking into military and PacBell computers;
- allegedly used phone phreaking techniques to interfere with radio station call-in lines, allowing him and his confederates to win thousands of dollars of prizes in contests, including cars;
- o maximum penalties up to 100 years imprisonment.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Links to Internet to be limited by DoD

Bob Kolacki <kolacki@itd.nrl.navy.mil> Mon, 10 Jan 94 16:41:36 EST

PRODIGY(R) interactive personal service 01/10/94 2:36 PM

12:46 PM (ET) 1/10

Defense To Halt Milnet Hackers

NEW YORK--US defense officials, fearing computer hackers could invade their data networks, are moving to limit military links to Internet -- the backbone of the emerging information superhighway, a computer magazine said today. Network World said a plan to add a protective gateway or relay to the worldwide Defense Data Network--also known as Milnet--has touched off an uproar among computer users both in and out of the Pentagon.

A brief notice from the defense department's network planning group said introduction of the gateway was due early in 1994, the magazine said. So far the plan has not been implemented, and Internet users said today they still had direct computer links to the Milnet.

A spokeswoman for the Pentagon had no comment on the report, but said the department closely monitored computer security. "We are looking at ways to protect the network against hackers and viruses," she said.

Network World said critics of the plan argue the security relay can not handle the volume of electronic mail and data that now flows daily between

Milnet and Internet users around the world.

And they questioned why less drastic security measures, including so-called firewalls common to US industry, have apparently been rejected by the military.

(From Reuters)

[srivas <srivas@csl.sri.com>: Should we pitch FM to ISRO? :-)]

Tue, 4 Jan 94 10:24:39 PST

Article 1637 (1 more) in misc.news.southasia (moderated):

From: ramani@saathi.ncst.ernet.in (S.Ramani) Subject: India - Software Glitch Causes PSLV Failure

Sender: usenet@mnemosyne.cs.du.edu (netnews admin account)

Organization: NCST, Bombay Date: Tue, 4 Jan 94 13:18:57 GMT

Country - India

Source - Times of India, Bombay Edition, 4th Jan 94

Sent by - S. Ramani

Bangalore: A software error in the pitch-control loop of the onboard guidance and control processor led to the failure of the Polar Satellite Launch Vehicle's (PSLV) maiden flight, according to the expert's panel which probed the setback, reports UNI.

Their findings were released by the Indian Space Research Organization (ISRO) here on Monday.

The PSLV-DI failed after a smooth lift-off from the Sriharikota range on September 20, 1993.

Verify your backups

Louis Todd Heberlein <heberlei@cs.ucdavis.edu> Fri, 21 Jan 94 09:27:18 -0800

The message below, from managers of wuarchive.wustl.edu, is one with which readers of RISKS should be familiar. How many of us are in the same position?

For those of you who don't know, wuarchive.wustl.edu is one of the largest and busiest Internet public archive sites, accessible via anonymous FTP and other means.

----- From /README.NOW in wuarchive.wustl.edu -----

The entire archives were destroyed the afternoon of Thursday, January 13th due to a bug in the system crash dump routines. There have been serious problems restoring backups due to a failed tape drive -- we have gotten a loaner drive, but there may not be any recent viable backups of the archives.

Translation: everything was lost, the archive maintainers are scrambling to find copies of all of the missing files -- it's probable that some files were lost permanently.

Thanks for your patience,

The Management

Safety in Telescript

"Luis Valente" <luis_valente@genmagic.genmagic.com> 17 Jan 1994 20:09:29 -0800

Phil Agre's message of January 6th ("Wild agents in Telescript?") brings up some very good points. In this message I would like to describe some of the safety features of Telescript that are used to prevent both ill-intentioned scripts (e.g., worms, viruses) and buggy scripts from damaging a Telescripted network.

- 1) The Telescript language is interpreted, rather than compiled. Thus, Telescript programs cannot directly manipulate the memory, file system or other resources of the computers on which they execute.
- 2) Every Telescript agent (i.e, Telescript program that can move around a Telescript network) is uniquely identified by a telename. A telename consists of two components: an authority which identifies the "owner" of the agent (e.g., the Personal Communicator from which it originated) and an identity which distinguishes that agent from any other agent of the same authority. The authority component is cryptographically generated and cannot be forged. Thus, when an agent is transferred from one Telescript engine to another, it is possible to verify (using cryptographic techniques) that the agent is indeed of the authority it claims to represent. (N.B.: a Telescript engine is a program capable of interpreting and executing Telescript programs).
- 3) Every Telescript agent has a permit which limits its capabilities. Permits can be used to protect users from misprogrammed agents (e.g., an agent that would otherwise "run away" and consume resources for which the user would have to pay) and to protect Telescript service providers from malicious agents. Two kinds of capabilities are granted an agent by its permit. The first kind is the right to use a certain Telescript instruction, e.g., the right to create clones of itself. The second is the right to use a particular Telescript resource and by which amount. For example, an agent is granted a maximum lifetime, a maximum size and a maximum overall expenditure of resources (called the agent's allowance), measured in teleclicks. An agent's permit is imposed when the agent is first created and is renegotiated whenever that agent travels to an engine controlled by a different administrative authority. If the agent exceeds any of its quantitative limits, it is immediately destroyed by the Telescript engine where it is executing.
- 4) Telescript agents move around a Telescript network by going from one

Telescript place to another. Telescript provides an instruction -- go -- that gives agents this travelling capability (if granted by their permit, of course). Places are Telescript programs in their own right. Before accepting an incoming agent, a place can examine the agent's telename, permit and class (N.B.: an agent represents an instance of a Telescript class; thus, the class of the agent represents the "program" that the agent executes. Like authority names, class names cannot be forged). Based on that information, the place can do any the following:

- a) Do not allow the agent to enter.
- b) Allow the agent to enter but only after imposing upon it a permit more restrictive than the one it currently holds (e.g., the agent is only allowed to consume 100 teleclicks while in this place).
 - c) Allow the agent to enter and execute under its current permit.
- 5) When a Telescript process (agent or place) interacts with another Telescript process, the telename and class of the former is available to the latter. This enables Telescript applications to control who can interact with them and in what ways.

I hope this (brief) description of some of the more pertinent security features of Telescript will help Risks readers understand how we've addressed the issues raised in the NYT article and in Phil's message.

-Luis Valente, General Magic, Inc.

Slippery Folks in the Oil Business

Peter Wayner <pcw@access.digex.net> Thu, 6 Jan 1994 15:48:48 -0500

Folks who are interested in the extent of industrial espionage (and thus the need for secure networks and secure encryption) will want to check out the lead story in January 6,1994 edition of the Wall Street Journal.

The details are more arcane than even the best spy novels, but the highlights are:

- * Information brokers would contact companies in the oil business and offer to "help" them win contracts for a percentage. They provided information gained through shmoozing and buying off insiders as part of their help.
- * Illicit payments reported in the story paid to the industrial spies ranged from \$10,000 to \$600,000. The contracts were worth \$100 million and up.
- * The Swiss government refuses to disclose information about the accounts where the loot is deposited because it says that this sort of behavior is not against the law in Switzerland.

Risks of Domain Names

Matt Cohen <Matt.Cohen@chron.com> Tue, 18 Jan 94 16:29:10 CST

At the end of December, after NBC Nightly News announced an address for Internet email - "nightly@nbc.com" - I wondered if the other US television networks had also established an Internet presence. A quick check of the Domain Name Service revealed the existence of "abc.com", "cbs.com", and "fox.com".

A search in the InterNIC registration database showed that none of these represented the organizations I would normally associate with those names. Instead of TV networks, I found a design firm, a consultant, and an online service.

The obvious risk is that of mistaken identity.

Less clear is the impact that such "misleading" email addresses may have on the way people do business. Increasing numbers of people do much of their professional interaction via email. Email addresses are appearing on business cards and becoming as accepted as postal addresses. The domain name portion of an email address is coming to represent an organization.

Domain names are given out on a first-come-first-served basis. This raises several questions. Will large companies consider "misleading" domain names to violate their trademarks? Will "misleading" domain names matching those or large companies be registered with the intent of receiving compensation for them when the companies eventually come on the Internet?

Not all the networks have been lagging behind, by the way - the Public Broadcasting Service ("pbs.org") has been on the Internet for over a year.

[By the way, I chided Matt for having such an amorphous net address. The "chron" gets grandfathered because of its early access to the Internet, and is actually the Houston Chron. PGN]

Re: Mail forwarding as easy as Call forwarding

John M. Sulak <sulak@blkbox.COM> 12 Jan 1994 03:10:05 GMT

>Has anyone ever tried to have 1600 PENNSYLVANIA AVENUE forwarded?

Yes. In January of last year, much of its mail was forwarded to Houston, Texas. :-)

Cellular phone security features...NOT!

Goldman of Chaos -- postmaster CRI-US <goldman@orac.cray.com>

Thu, 20 Jan 94 10:37:25 GMT-5431:28

Last night I purchased a Cellular phone. While reading through the manual I found a section labeled "Security features" Neat. The manual talked about two security codes, a 3 digit number to unlock the phone and a 6 digit number that is used to change the unlock number and a number of other security features. The 6 digit number can also be used to unlock the phone. The 6 digit number is not easily reprogrammed.

The 3 digit number was included with the documentation; however, I couldn't find the 6 digit number. So I called the technical help line. Their answer floored me. "The 6 digit number is '123456', '654321', or all zeros. Just give one of them a try." So much for security.

The manual did state that a different 6 digit number should be chosen for each phone. Sigh.

Matthew Goldman E-mail: goldman@orac.cray.com Work: (612) 683-3061

Harvard Case of Stolen Fax Messages

Sanford Sherizen <0003965782@mcimail.com> Thu, 20 Jan 94 08:19 EST

This is dated but worthwhile for readers of RISKS. The Boston Globe of December 15 published an column by Alex Beam about an academic battle over the Harvard Semitic Museum. The Museum has an outstanding collection but was recently closed down, leading to very public battles involving many celebrities. What caught my eye in Beam's description of the controversy is the following quote:

"Stager (the museum's director) instructed his secretary to remove used fax cartridges from the trash, unravel the carbonized ribbon and reconstruct the staff's facsimile transmissions, to monitor surreptitious fund-raising> (This little trick won't work on modern laser-printed fax machines, in case you're getting any ideas.)"

"Stager 'talked to the (Harvard) general counsel's office, and asked them if it was against the law," his assistant, Eileen Caves, told the Harvard Crimson. They 'classified the carbon as "abandoned material that was left in a public place" and said it was therefore public information."

Risks? It may have happened at Harvard, it may be possible to reconstruct messages, and it may be why lawyers should be buried 35 feet underground since, deep down, they are very nice people.

Sanford Sherizen, Data Security Systems, Natick, MA

✓ Spontaneous recovery from "NOMAIL" setting?

Ron Ragsdale <R_RAGSDALE@oise.on.ca> Fri, 21 Jan 1994 15:13:39 -0500 (EST)

Setting "NOMAIL" to leave a LISTSERV keeps open the option of an easy return, but it may also lead to an unexpectedly full emailbox. Early in January, I began receiving regular messages from a LIST that I had set to NOMAIL in 1991; the LIST owner told me I was set to NOMAIL, but messages only/stopped when I sent an UNSUBSCRIBE message. Earlier this week (JAN. 16), I received my first update from RISKS in several years, under the same conditions, with my membership set to NOMAIL. Today, I received 80 messages from a LIST I had left (through NOMAIL) about four years ago and quickly sent an UNSUBSCRIBE message (which was acknowledged).

A student of mine has been doing research on a number of lists and a substantial fraction of the respondents tell about similar phenomena? Is the NOMAIL setting really a time bomb that may flood your mail directory unexpectedly? (I was fortunate in TELNETing from Berkeley today just as the avalanche had begun.) If you have an explanation of this process, I would appreciate hearing it.

Ron Ragsdale, Professor Emeritus, Ontario Institute for Studies in Education 252 Bloor Street West, Toronto, Ontario, Canada M5S 1V6 (416) 923-6641 X2252

★ Re: Hacker nurse makes unauthorised changes to prescriptions

Li Gong <gong@csl.sri.com> Thu, 20 Jan 94 18:08:08 -0800

In <u>RISKS-15.37</u>, John Jones quoted The Guardian (21st December, 1993)'s report on the conviction of a male nurse who hacked into a hospital's computer system and modified entries, including prescriptions.

Tow or three weeks back, the Guardian Weekly (probably in its Le Monte section) reported the widely spread practice (in may parts of the world) of illegally obtaining human organs for reselling to transplant patients. Among the many methods (such as kidnapping), one is to simulate heart failure on the monitoring machines in hospitals.

Li Gong, Computer Science Lab, SRI International, Menlo Park, California

Proposal for new newsgroup on safety-critical systems

<jdm@minster.york.ac.uk> Fri, 21 Jan 94 10:00:00

Proposal for new newsgroup on safety-critical systems Comments please, to news.groups.

Proposed name: comp.safety or comp.safety-critical or comp.risks.safety ...

Charter

A forum for discussion of the engineering and assessment of safety-critical systems, with special reference to computing.

Moderated group - Proposed moderator:

Jonathan Moffett (jdm@minster.york.ac.uk)

Senior Research Fellow in the High Integrity Systems Engineering Group Department of Computer Science, University of York, York YO1 5DD, England

Tel: +44 (0)904 432788, Fax: +44 (0)904 432767

Discussion

The newsgroup would be a forum for discussions about systems safety which could afford to be more detailed than comp.risks and more specialised than comp.software-eng. It would cover safety requirements and risks, safety engineering techniques and safety assessment. Its focus would be on safety-critical computer systems and computer-supported design and assessment of general system safety.

There is no newsgroup at present which deals specifically with systems safety - in a search through the Usenet postings about newsgroups the string "safe" appears only in rec.pyrotechnics, alt.irc.corruption and warnings about humor.

There is of course comp.risks, with which the new group would overlap but not compete; comp.risks is wider in scope than safety, and is not very much used for technical discussions. There would also be overlaps with: comp.software-eng, which is a very high-activity group of which safety issues are a very low proportion; and comp.specification[.z], because of the indirect relationship (via high assurance) between formal specification and safety. Other possible overlaps are comp.realtime and comp.human-factors.

There appear to be a gap in the market which a safety newsgroup could fill.

It should be moderated, because safety is a very sensitive issue, subject both to flaming :-) and hoaxes.

[A SAFE bet! The proposal sounds like a good idea. Be sure to send your comments to jdm and news.groups, but CC: RISKS if you like. PGN]

Privacy Digests

Peter G. Neumann <Neumann@csl.sri.com> Wed, 5 Jan 94 13:33:37 PST

Periodically I will remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry general discussions in which risks to privacy are a concern.

* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the

full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@vortex.com"; you will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Leonard P. Levine. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated) forum, and was established 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. Submissions should go to comp-privacy@uwm.edu and administrative requests to comp-privacy-request@uwm.edu.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing detailed discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN

✓ ISSA Conference Announcement

<davelenef@aol.com> Thu, 13 Jan 94 00:20:57 EST

TO THOSE WITH RESPONSIBILITY FOR -- OR AN INTEREST IN -- INFORMATION SECURITY:

The Information Systems Security Association (ISSA) is holding its 11th Annual Conference and Trade Show, March 13-17, 1994, at the Fairmont Hotel in San Francisco, Calif.

This info-security conference will feature 72 educational sessions divided among the following tracks: Network, Distributed and Client/Server, Management, Technical, Government/Legal, Audit, Awareness, and Business Continuity. Major security vendors will exhibit at the ISSA trade show. There will be a tour of Silicon Valley corporations.

The following industry experts will present addresses: Harry Saal (Network Data General) -- The Super Digital Highway; James Settle (FBI) -- computer crime investigation; and Gail Warshawsky (Lawrence Livermore) -- computer security awareness.

For an advance program, registration information, and ISSA membership information, please contact ISSA Headquarters at 312/644-6610 x3410 (voice),

or 312-321-6869 (fax). Mention where you saw this notice!

EARLY BIRD DISCOUNT IF REGISTRATION POSTMARKED ON OR BEFORE 1/31/94.

Dave Lenef, Marketing/Communications Coordinator Information Systems Security Association (ISSA) 312/644-6610



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 40

Monday 24 January 1994

Contents

Re: Spoofing Air Traffic Control

John Stanley

Wolper

Re: Spoofing Telescript

Barry Margolin

Adrian Howard

Paul Barton-Davis

Geoffrey Speare

John Pettitt

Re: Spoofing SETI

Someone at NASA?

Bear Giles

Mark Staltzer

Steven King

Steve Elias

Charles Bryant

David Honig

Mark Thorson

Jon Mauney

Andrew Klossner

Dan Keith

Adam BJ Quantrill

Info on RISKS (comp.risks)

✓ phony air traffic controller (Pereira, RISKS-15.39)

John Stanley <stanley@skyking.oce.orst.edu> 22 Jan 1994 00:01:21 GMT

>This raises interesting questions of authentication. Wouldn't it be possible >to add to air traffic messages some kind of ``signature" that would help >receivers distinguish between legitimate and bogus messages?

If there were to be such a voice authentication system, the information would

need to be readily available to every pilot. This includes not only those who fly for large commercial airlines, but to every private (even student) pilot. Any pilot who might use air traffic control (ATC) facilities would need to know this data, and there are several hundred thousand of them. In addition, for the same reason that visual flight rules (VFR) pilots must carry aeronautical charts for the area they fly in, they would need to have the authentication codes for the whole area. (In an emergency, you might wind up at ANY airport within the flying radius of your airplane, especially if that emergency was because you weren't where you thought you were.)

If the information is that readily accessible, the bad guys can get it, too.

An additional concern is that the airport vicinity is often not the place where you want to require from pilots the extra effort (or time) required to look up authentication codes before they follow instructions.

Some of this problem may be solved by the use of digital printed data, which are in use in some aircraft. This will not filter down to the private aircraft for many years.

Re: phony air traffic controller

Jim Wolper (research) <wolperj@pequod.isu.edu> Mon, 24 Jan 94 10:35:59 -0700

Fernando Pereira makes the suggestion of adding a ``signature'' to air traffic control messages as a means of verifying their authenticity. This is an interesting suggestion. The comments below relate primarily to the Air Traffic Control (ATC) system in the US.

The present system of air-to-ground communication has two components: VHF voice and UHF radar transponders. Currently, aircraft flying under Instrument Flight Rules (under which all air carriers and many supplemental carriers are required to operate) carry a transponder which is capable of replying to a radar sweep with a 12-bit identification code and its altitude. This is referred to as a "Mode C" transponder. It would be very difficult to construct an unspoofable authentication code for either of these systems.

The FAA has plans to upgrade to ``Mode S" transponders, which would give ATC a digital uplink capability. This would make it easier to implement a verification code, but I have no idea whether this issue has been discussed by the FAA.

The original date for adoption of the Mode S standard was 1992, but there has been quite a bit of slippage. Mode S transponders will be much more expensive, of course, and smaller aircraft (both personal and corporate) will probably continue using Mode C transponders and voice communication for some time.

Jim Wolper, Certificated Flight Instructor, Department of Mathematics Idaho State University Pocatello, ID 83209-8085 USA

Safety in Telescript

Barry Margolin <barmar@Think.COM>
Sun, 23 Jan 94 17:30:18 EST

>1) The Telescript language is interpreted, rather than compiled. Thus, >Telescript programs cannot directly manipulate the memory, file system or >other resources of the computers on which they execute.

Don't forget: that's what we all thought about fingerd. RTM, Jr. showed us to be wrong.

And even ignoring bugs like this, interpreted vs compiled isn't the real issue. Postscript is typically interpreted, but since it has operators that access files and can manipulate the interpreter's standard dictionaries, virii can be implemented with it.

Some of the access control features described may prevent these kinds of intrusions, but until we see more details I think we are be justified in being concerned.

Barry Margolin, System Manager, Thinking Machines Corp. barmar@think.com {uunet,harvard}!think!barmar

RE: Safety in Telescript (Valente, RISKS-15.39)

"Adrian Howard" <adrianh@cogs.susx.ac.uk> Mon, 24 Jan 1994 11:41:18 +0000 (GMT)

>1) The Telescript language is interpreted, rather than compiled. Thus, >Telescript programs cannot directly manipulate the memory, file system or >other resources of the computers on which they execute.

This is a bit of a red-herring. Just because a language is interpreted by no means implies that it cannot be used to produce worms/viruses. I have seen viruses in Unix Shell scripts and even BASIC programs! IMHO it is *far* easier for the average malicious idiot to produce a virus in a decent interpreted scripting language than by hacking around with compiled executables.

The face that Telescript programs "cannot directly manipulate the memory, file system or other resources of the computers on which they execute" must be due to restrictions in the design of the language. They have nothing to do with compiled vs interpreted programming. If an agent has the capability to alter itself/other agents, it has to be manipulating the memory etc of the computer it is executing on.

>2) Every Telescript agent (i.e, Telescript program that can move around a >Telescript network) is uniquely identified by a telename. A telename >consists of two components: an authority which identifies the "owner" of >the agent (e.g., the Personal Communicator from which it originated) and >an identity which distinguishes that agent from any other agent of the

>same authority. The authority component is cryptographically generated >and cannot be forged. [...]

I presume you are going to give some information on the algorithm used for producing the unique "telename" so we can feel a little more sure about the "cannot be forged" bit :-) Also, does the telename change for self-modifying agents (if such things can be produced with Telescript?)

>3) Every Telescript agent has a permit which limits its capabilities.
>Permits can be used to protect users from misprogrammed agents (e.g., an >agent that would otherwise "run away" and consume resources for which the >user would have to pay) and to protect Telescript service providers from >malicious agents. [...]

I am presuming that "permits" (why not "telepermits" :-) are also encrypted in some way to prevent naughty people producing agents which fib about what they are allowed to do. Like Phil Agre, I too am "looking forward to the first few reverse-engineered Telescript products"!

[Disclaimer: I have to admit my entire knowledge of Telescript comes from the two RISKS articles I've read, so apologies for the picky tone. To the peeps at GM, I do find the concept of an agent scripting language fascinating, and it's good to know that you are thinking about security issues.]

adrianh@cogs.susx.ac.uk

✓ Safety in Telescript

Paul Barton-Davis <pauld@cs.washington.edu> Mon, 24 Jan 1994 10:09:21 -0800

Luis Valente < luis_valente@genmagic.genmagic.com> writes, in connection with Telescript:

1) The Telescript language is interpreted, rather than compiled. Thus, Telescript programs cannot directly manipulate the memory, file system or other resources of the computers on which they execute.

Since we all know that sh, BASIC, awk, perl and tcl are completely free of security holes, we can know feel at ease knowing that, since Telescript is interpreted, and thus cannot "directly manipulate the memory, file system or other resources", Telescript is safe as houses.

Presumably the reason that C is less safe is that it can "directly manipulate" [sic] the filesystem of a computer.

```
echo foo > bar;
{ printf ("foo\n") > bar }
fd = open ("bar", O_RDWR); write (fd, "foo\n", 4);
-- paul
```

✓ Re: Safety in Telescript

Geoffrey Speare <geoff@omg.org> Mon, 24 Jan 1994 13:49:23 -0500

- > The authority component is cryptographically generated and cannot
- > be forged.

As a regular RISKS reader, this sentence alone tells me all I need to know...

(It sounds like General Magic is taking reasonable precautions against "ill-intentioned scripts", which of course means that dedicated people will be able to create such scripts anyway, and that some sites will be more vulnerable than others.)

Geoff Speare, OMG, geoff@omg.org

★ Re: Safety in Telescript

John Pettitt <jpp@netcom.com> Mon, 24 Jan 1994 19:00:54 -0800

Luise Valente of General Magic writes: [about telescript]

>1) The Telescript language is interpreted, rather than compiled. Thus, >Telescript programs cannot directly manipulate the memory, file system or >other resources of the computers on which they execute.

Pardon? Since when has an interpreter been safer than a compiler? Any programming language capable of useful work is also capable of destruction. [this is known in our office as "Pages law of languages" after John Page who says it repeatedly]

Valente the goes on to further document how cryptographic (presumably public key) signatures are used to ensure secure and limited processing of agents.

However the asserts that forged messages are impossible, that is a very brave thing to say in the light of the history of such statements.

Several questions spring to mind:

- 1) will the security be published and subject to external verification (see all the arguments about clipper)?
- 2) will the security be downgraded for export, if so could a compromised 'export' message run on domestic networks?
- 3) what is the vulnerability to social engineering? As has been proven people are always the weak link.

4) what provision will there be to stop re-chipped / 'tumbled' devices?

I for one would be far happier with some clear discussion of risk rather than the classic "it can't happen response" we see so regularly until it does happen.

John Pettitt - Email: jpp@netcom.com or jpettitt@well.sf.ca.us

Phone: 408 236 3202 Fax: 408 241 0307

✗ Low risk of alien virus from receiving SETI signals

<SYSTEM@LOWGMO.LARC.NASA.GOV> Mon, 3 Jan 1994 13:58:07 -0500 (EST)

The initial risk level from alien signals is very, very low. Since the hostile intelligences can not know the details of our computer systems, writing any kind of virus would be very nearly impossible. Indeed, achieving any kind of communication would be (will be?) very difficult. The few tests that have been conducted so far involve one scientist composing a message based on "universal" mathematical constants and relations. Usually this message is to be laid out in a square matrix, with stick figures of a human, blobs for our solar system, etc. Unfortunately, often other scientists can not decipher the message. Now consider that the intelligences trying to decipher the message might be a squid living 20 miles down in a Jovial type atmosphere. Also note that it took humans 10K years or so to discover that by using sign language they could communicate with monkeys.

Next, communication will take a LONG time. Since we have been listening for a few years now, it is reasonably certain that we have no technologically advanced nearby neighbors, that is within 50 light years or so. So our hostile alien will have to guess the detailed operation of the computer(s) we will be using 50 or 500 years in the future when his message gets here.

A certain amount of risk does exist. If the aliens are very much more intelligent that we are (possible with genetic engineering or more efficient evolution) and we develop extensive communications with them (hoping for some crumbs of their superior technology) then when they send a wonderful program for us to run with root privilege.... A very much worst case is given in "A Fire Upon the Deep" by Vernor Vinge where billions of worlds are destroyed by hostile programs via the galactic equivalent of the internet.

The bottom line is, after we gain some reasonable level of communication with the whatevers, be very wary of Greek gifts, and/or offers of alien waterfront property.

Can SETI signals bear viruses?

Bear Giles <bear@tigger.cs.colorado.edu> Mon, 3 Jan 1994 14:25:43 -0700 Is this a reasonable assumption? We've always sent "baby talk" messages, but then again we've sent very short messages. And we're barely a technological civilization; we've had radio for a century, computers for half that. Many people living today were born before the first digital computer was built!

What about a society willing to run a sequence which contained a few terabytes of information, starting from a simple binary raster image and progressing to fractally compressed images (or an even more advanced technology) and possibly even a DNA dump? Can we really assume that SETI signals will be pure "data", and not the equivalent of a 9 track containing uncompress.c in plaintext, tar.c.Z, and then encyclopedia.tar.Z?

(This is not an idle thought; a while back someone posted a bogus "SETI" signal to sci.crypt. It contained a primer in digital logic and could have easily been extended to give the specification for a computer.)

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

Re: Can SETI signals bear viruses?

<stalzer@macaw.hrl.hac.com>
Mon, 3 Jan 1994 15:23:16 +0800

Not to worry, if alien programmers are anything like human programmers, their viruses must contain bugs. Besides, I doubt any other species could create sendmail.

-- Mark

[Actually a much greater risk exists of April Fool's Spoofs coming from people on this planet. But the ultimate hoax would be one cleverly created by alien intelligence. PGN]

✓ Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

Steven King, Software Archaeologist <king@wildebeest.cig.mot.com> 4 Jan 1994 22:06:56 GMT

Several people have refuted the idea of SETI signals containing a virus, but I'm not sure anyone has really explained *why* this isn't a problem. At least, I don't think there's been enough of an explanation for the lay-person who's view of computers has been molded by one too many episodes of Star Trek...

Viruses are computer programs. Nothing more, nothing less. The have the property of being able to replicate themselves and, through crafty programming, "infect" other computers. What do I mean by "infect"? Simply that the programmer has found a tricky way for the program to get transferred to another computer without the operator being aware. This usually involves the virus hiding itself somewhere on a disk or in another program.

Just like any other program, a virus must be run in order to be effective.

Obviously the operator won't knowingly run a viral program. The virus's programmer uses a trick of the particular computer to force the virus to be run. Say the virus attaches itself to another program. It'll do this in such a way that when the operator thinks he is starting the benign program, he's actually starting the viral program. This can be done with varying degrees of sophistication, of course. As another example, say the virus writes itself to a boot disk. The virus's programmer will typically make it install itself in place of part of the operating system, so the virus is run instead of (or in addition to) the computer booting.

So, the virus is just a program. It must be run. And, like any other program, it can only be run on a particular brand of computer. You can't run Macintosh programs on an IBM, and you can't infect an IBM with Macintosh viruses. (We'll ignore emulation programs like SoftPC for the purposes of this article.) Viruses aren't effective until they're run. You don't need to worry about spreading viruses if you transfer data disks (say, word processing or spreadsheet files) between computers. Viruses aren't *DATA*, they're *PROGRAMS*.

In order for a SETI virus to be effective it must be run as a program. We're not doing that with SETI signals now, and I doubt we ever will. For one thing, what sort of computer would we run the SETI program on? I really doubt the Little Green Men use IBM compatible computers! Or any other sort we commonly use here on Earth. Even if there were a computer program (viral or benign) contained in the SETI data we'd have no way to execute it without an alien computer. This is the real reason we're safe. Even if the data stream contains a viral program we'd need to run it in order for it to be effective. And to run it we'd need the alien's computer.

Okay, let's say we have some *REALLY* malicious Little Green Men out there. They've beamed up a 486 machine and have written a virus for it. They send the viral program down so our SETI antennas pick it up. The researchers here miraculously recognize 486 machine code in the data stream and run the program. Are we dead? Well, hopefully if it comes to that one of our Heroic Scientists will have the presence of mind to read the bloody code before they run it! Or at least, they'll run it on a machine that's not networked to anything. Of course, if the aliens are capable of this in the first place they can probably do a lot worse to us than writing silly little computer viruses.

Steven King -- Motorola Cellular Infrastructure Group

can SETI signals bear viruses

Steve Elias <eli@cisco.com> Wed, 05 Jan 94 17:06:25 PST

Oh, that we really might have an opportunity to worry about picking up anything at all with SETI, never mind programs containing viruses or Super Mario Brothers 32767.

Didn't congress just cancel funding the latest and very great SETI project

that had only recently begun?

[Yes, but various private sources are keeping it going. PGN]

Re: SETI viruses

Charles Bryant <ch@hk.net> Thu, 6 Jan 94 16:03:43 HKT

There is an assumption in this discussion that a virus received by SETI would need a particular type of hardware to run (i.e. an electronic computer). It is possible, however, that it could use the human brain instead. This could happen either at an individual or a group level.

At the individual level, most people have experienced a persistent tune which, once heard, almost forces them to hum it for some time afterwards. Imagine a more powerful effect where hearing the tune hummed by someone else is enough to propagate the effect.

At the group level, consider Communism. From the number of countries which have tried it, it is clearly an idea that sounds correct initially, even if practical application proves less successful. We are obviously spreading this particular virus in TV and radio broadcasts which are spreading off into space continuously.

There is also an assumption that a virus must be harmful. This is not necessarily so -- the only true characteristic of a virus is that it can only reproduce by using its host and a virus which helps its host might be more successful in some circumstances. In particular, if interstellar communication is greatly helped by a virus, such a virus would be much more likely to be received here than one which debilitates a civilization.

Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

David Honig <honig@ruffles.ICS.UCI.EDU> Thu, 06 Jan 1994 12:28:54 -0800

... since the nearest star is 4 light years away, the operating system they developed for would be obsolete by that time...

Although if they broadcast 8088-compatible virii...

Re: Can SETI signals bear viruses?

<mmm@cup.portal.com>
Thu, 6 Jan 94 21:03:39 PST

Although a computer virus passed through SETI seems unlikely, a human virus is not. If a book like the Bible, Dianetics, or Das Kapital were received, it

could cause enormous harm. Instantly, large numbers of people (albeit slightly loony people) would see it as important received knowledge, perhaps even holy knowledge, and begin to act accordingly.

The defense is obvious. We must beam copies of our most dangerous books into space. This will subvert and destroy alien societies before they have a chance to do the same thing to us!

Also, we must evaluate the threat. Government scientists should set to work on developing the most "effective" stories possible, to see how dangerous they can be. Of course, this work would have to be extremely secret to prevent its accidental release.

Mark Thorson (mmm@cup.portal.com)

★ Re: Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

Jon Mauney <mauney@adm.csc.ncsu.edu> Tue, 4 Jan 1994 14:24:55 GMT

This in turn sounds similar to Piers Anthony's "Macroscope" in which the recently-discovered-on-earth macron particle turns out to be a great communications carrier, and supports a sort of intergalactic Usenet. But most of the channels are jammed by a brain virus: access the information and you go nuts.

Probably a lesson there for us :-)

Jon Mauney, Mauney Computer Consulting mauney@csc.ncsu.edu (919) 828-8053

[Also noted by Bruce Grant (bgrant@umcc.ais.org), although the intended target was sentient beings rather than machines. PGN]

Re: Can SETI signals bear viruses?

Andrew Klossner <andrew@frip.wv.tek.com> Mon, 3 Jan 94 12:31:16 PST

Some ideas about malicious agents within SETI data have been explored in depth in science fiction. One scenario goes like this: aliens send us terabytes of scientific and engineering data, including plans for constructing wonderful devices. We construct those devices and deploy them massively. The aliens invade, and activate a trojan horse in the devices. This plotline was used in "The Ophiuchi Hotline" by John Varley.

-=- Andrew Klossner (andrew@frip.wv.tek.com)

★ Re: Can SETI signals bear viruses?

Dan Keith <tellab5!odgate!dbk@uunet.UU.NET> Fri, 7 Jan 1994 00:20:44 GMT

There was a science fiction novel by astronomer Fred Hoyle called "A for Andromeda" (and a sequel, "Andromeda Breakthrough"). In the story, a SETI-like listening program detects signals from the Andromeda Galaxy. These are eventually decoded into instructions for a computer and its program. The computer is built, at which point it then builds an android which becomes the protagonist. The rest of the story doesn't have much bearing on the discussion, though.

Dan "Bud" Keith dbk@odesta.com

★ Re: Can SETI signals bear viruses? (Cantillo, RISKS-15.36)

Adam BJ Quantrill <adam@kbss.bt.co.uk> Fri, 7 Jan 94 15:50:36 GMT

... but taking a Star Trek TNG episode as an example (!), the scientists were all too willing to find any way at all to run a genetically buried program on their computer. Presumably a scientist would try to build an emulator to run the opcodes. Are the SETI scientists sufficiently careful in their approach to build an emulator that could not be subverted by the 'executable' it runs?

- Adam



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 41

Weds 26 January 1994

Contents

Lightning on the Ethernet

eddy

not flo

E-Mail Fraud

Lori Carrig

Update on voter fraud in Costella County, Colorado

Bear Giles

Laptop Computer Could Explode

F. Barry Mulligan

Opening of European borders delayed by InfoSys problems

Bertrand Meyer

Canada loses satellites -- anyone have more info?

Alan Wexelblat

Risks of dynamic binding

Andrew Shapiro

New museum on cryptography

Jeremy Epstein

Is Global Authentication Impossible?

Li Gong

Re: Phony air traffic controller

Mark A. Bowers

Cameron Strom

Re: Smart Cars and Highways

Jerry Leichter

Telescript risks

Bob Blakley III

Re: Can SETI signals bear viruses?

Andrew Klossner

Info on RISKS (comp.risks)

Lightning on the Ethernet

eddy <eddy@gen.cam.ac.uk> Wed, 26 Jan 94 16:10:01 GMT We had our local unix-support by yesterday helping us out with a putative kernel reconfiguration; told me the following job after which he'd had to do the sorting out recently:

The two principal departments of Maths here, pure and applied, face each other around a courtyard. Someone had bunged an ethernet link out the window of one and in the window of the other in order to get their PC in one attached to the ethernet in the other.

When, in due course, we had a thunderstorm, the PC and the ethernet box on the other end of the link were both totally cooked. Fortunately, the damage stopped there. Let's hope they now stick in a gateway to connect the two departments so no-one will try that again.

Eddy

[and not Flo. Yes, An Eddy is of course a current running opposite to the normal flow. PGN]

E-Mail Fraud

Lori Carrig <carrigl@fire.nic.ddn.mil> Wed, 26 Jan 1994 13:15:34 -0500 (EST)

Electronic Mail Fraud, by Lori Carrig

With the advent of Electronic Mail we have several risks associated with this modern vehicle of information. Of these risks one is E-Mail fraud. Just like with Mail and Telephone fraud, Electronic Mail fraud has come of age. Before I diverge into this problem let me set an example of an incident I worked on:

I received a notice from a user that she received E-Mail promoting computer chips for sale from a internet address. She had not received her items which she paid for and wanted to report it. She gave the following account:

She had received and responded to this address about the sale of the described items. After several exchanges of E-Mail from the culprit the price was determined and she inquired to the method of payment for the desired items. The culprit explained that they would only take Money Order. The culprit would accept a check, but would not ship the desired items until after the check has cleared. A name and address was given, but no phone number, to send the check to. The culprit stated that they would ship the items after 5-7 days. After 9 days the victim sent an E-Mail message to the culprit and inquired if they received the check. A message was sent back stating that they did receive the check and was awaiting for it to clear the bank. After 30 days the victim had not received the ordered, and paid for, items from the culprits.

The risk here is quite apparent. As with Mail and Telephone Fraud, E-Mail fraud can cause extreme losses to users. What would prevent such an incident? Well here are some of the ways I have seen:

- 1. Order from known companies like Intel, Microsoft, CompUSA, and so on.
- Pay with an Credit Card. You have the right to cancel the payment within 30 days if the items have not been received. There is other risks associated with giving you Credit Card number out, but I will not address them at this time.
- 3. Request a phone number and call the vendor to confirm the order.

The best prevention is number 1 above and common sense. Know who you are dealing with before any monetary exchange takes place. Items 2 and 3 above have other risks involved with them which, in turn, may be another form of fraud.

There are other samples of E-Mail fraud, but I will not address them at this time. I will leave that for future releases. With the estimated losses to Computer crime ranging from \$3-6 billion dollars(1) it is cause for alarm.

If you suspect that you are a victim of E-Mail fraud, contact your local police department. Please note that only 11% of computer crimes are ever reported to law enforcement.(2)

The opinions above are mine only and DO NOT reflect any other parties position.

Lori Carrig carrigl@nic.ddn.mil

Footnotes:

(1) Publisher: Search, Sacramento, CA

(2) Publisher: Law and Order, September 1990

Update on voter fraud in Costella County, Colorado

Bear Giles <bear@tigger.cs.Colorado.EDU> Wed, 26 Jan 1994 10:19:50 -0700

[Followup on election fraud report from last summer (fall?).]

A state grand jury in Denver has indicted eleven people for voter fraud in Costella County, Colorado. In 1990, the census found 2278 adults living in the county, but there were 2536 registered voters.

Those indicted include:

- o County Clerk Roy David Martinez, charged with falsifying residency reports in the 3 November 1992 general election.
- o His wife, deputy clerk and recorder Mariconsuelo Stella Rodriquez,

charged with allowing Martinez's sister, a non-resident of the county, to vote

- o Costella County Commissioner George Valdez, charged with aiding and abetting voter fraud, threatening to withhold a county employee's pay unless he voted for Valdez, and enabling a jail inmate to vote absentee, all during the August 1992 primary.
- o former County Commissioner Ernest Leo Chavez, charged with helping an alien to vote absentee.

Also indicted were former County Commissioner Samuel Gonzales and his wife Lisaida, Martinez's siter and brother-in-law, two sisters-in-law of George Valdez and one of the latter's husband.

Lisaida Gonzales was registered to vote in both Costilla and El Paso [Colorado Springs] counties. The relatives of George Valdez were registered in both Colorado and California since the 1940s.

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

Laptop Computer Could Explode

"F. Barry Mulligan" <MULLIGAN@ACM.ORG> Wed, 26 Jan 1994 06:01:21 -0600 (CST)

Source: Consumer Reports, Feb 94, p.125, "Recalls" column

NEC Technologies laptop computers; Battery could explode and catch fire.

Products: 13,000 computers, models PC-17-01 and PC-17-02, sold 12/88-4/90. Model no. appears on bottom.

What to do: Turn on computer with AC adapter disconnected and allow battery to discharge fully. Call 800 237-2913 for replacement battery and \$100 bonus.

(The image of a laptop exploding has a certain horrid fascination.)

/* barry /& mulligan@acm.org

Opening of European borders delayed by information system problems

Bertrand Meyer <bertrand@eiffel.com> Wed, 26 Jan 94 09:04:11 PST

Source: Agence France-Presse, 26 January 1994

The Schengen agreement stipulates the opening of borders between nine countries of the European Community (the Twelve minus Great Britain, Ireland

and Denmark). The agreement's implementation has already been delayed several times but was now planned for February 1st. A report of the French Senate's foreign affairs committee states that it won't be operational for another year. According to the chairman of the committee, Xavier de Villepin, the culprit is the computer information system, which is not yet "operational".

[This is a politically charged issue, because of fears regarding security (read terrorism) as well as illegal immigration from outside the European Union. I haven't seen any details about the problems of the "computer information system". -- BM]

-- Bertrand Meyer, ISE, Santa Barbara

Canada loses satellites -- anyone have more info?

"Alan (Miburi-san) Wexelblat" <wex@media.mit.edu> Wed, 26 Jan 94 10:33:03 -0500

This is from EDUPAGE, the summary service run for free by EDUCOM:

- > SATELLITES OUT. Geomagnetic storms caused by solar flares knocked out
- > Canada's two communications satellites within hours of each other.
- > Affecting broadcasters, phone and cable companies, and other business
- > subscribers, they began to question the reliability of satellite
- > communications in the context of the info-highway and examine more
- > land-based means of transmission. (Toronto Globe & Mail, 01/22/94 A1).

Does anyone have access to the original Globe & Mail article cited, or more info from another source? Did this loss of equipment mean interrupted or lost service, or did everything just switch to land lines?

When they say "knocked out," does that mean the satellite hardware is damaged, or just that the software got wiped?

--Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard, Media Lab, Adv. Human Interface Group wex@media.mit.edu 617-258-9168 an53607@anon.penet.fi

Risks of dynamic binding

Andrew Shapiro <shapiro@marble.Colorado.EDU> Wed, 26 Jan 94 14:40:49 MST

A quick description of dynamic binding:

When a program is linked (the object files are put together,) certain common routines (like the I/O calls) are copied from a standard library into the executable file. This is called static binding. Dynamic binding allows the library routines to be stored in one place and are joined with the executable only when it is loaded to run. Dynamic binding saves space and allows libraries to be updated without re-linking executables. They also can be deleted.

The other evening I stumbled upon an interesting single point failure for Sun

Microsystem computers. While working I distroyed the /lib/libc.so.0.15 file. To my surprise nothing works without it. I already knew that Sun's defaulted to dynamic binding at link time, I also knew that it was possible to suppress this option by using the -Bstatic keyword to the link editor, Id(1). What surprised me was that the static option had not been used when building any of the user commands. I would have expected some of the most basic commands like Is, cp, and either tar or dd to be compiled with static linking. If this were the case repairing the /lib/libc.so.0.15 file would be simple. Instead I was forced to reboot from tape, install the mini-kernel and then mount the filesystem and restore the file.

I believe the engineers that developed the dynamic binding system understood the implications of *every* program depending on a single file and kept the static binding option to prevent this. However, if the OS designers never use the static option and the dynamic library is lost . . .

Andrew T. Shapiro, CSES/CIRES University of Colorado, Campus Box 449 Boulder, CO 80309-0449 (303) 492-5539 andrew@gooter.metronet.org

New museum on cryptography

Jeremy Epstein -C2 PROJECT < jepstein@cordant.com> Tue, 25 Jan 1994 09:32:41 -0500 (EST)

There's absolutely no RISK in this article, but I thought it might be interesting to RISKS readers.

The 24 Jan 1994 *Washington Post* has an article about a new museum of cryptography at NSA. The author describes the runaround in trying to locate it, finding the usual problem of NSA phone numbers which answer with extensions and people who don't have names. The article then goes on to describe why cryptography is so important.

The museum contains all sorts of gems of the cryptography trade, including some old ciphering machines, displays of Civil War use of SIGINT, Enigmas (including one that can be tried out by museum visitors), and a Cray X-MP.

The museum is located in a building surrounded by barbed wire behind an old gas station near Baltimore. According to the author:

The National Cryptologic Museum, reached by exiting the Baltimore-Washington Parkway east on Route 32 and heading behind the Shell station, is open from 9am to 3pm Monday through Friday. Some at NSA say you can reach it at 301-688-5849. Others at NSA deny that number exists. I haven't been there (if it in fact exists :-), and would be interested in hearing from others if it's worth the trip.

--Jeremy Epstein Cordant, Inc. jepstein@cordant.com

[I'm sure some readers will find risks. BTW, for old-timers, it was the Colony 7 motel. I am told it is indeed open to the public. PGN]

Is Global Authentication Impossible? (Re: phony air traffic controller)

Li Gong <gong@csl.sri.com> Tue, 25 Jan 94 14:54:55 -0800

In RISKS-15.40, John Stanley (stanley@skyking.oce.orst.edu) argued:

If there were to be such a voice authentication system, the information would need to be readily available to every pilot. This includes ... several hundred thousand of them. In addition, ... If the information is that readily accessible, the bad guys can get it,

Contrary to this gloomy picture, past two decades of research in distributed computing, especially in naming and authentication, seems to suggest that (1) naming information can be made globally available and (2) authentication data can be widely distributed without compromising security (e.g., using public-key certificate technology).

Li Gong, SRI International, Computer Science Lab, Menlo Park, CA 94025, USA

Re: Spoofing Air Traffic Control

Etc Bowers <n911@pnet16.cts.com> Wed, 26 Jan 94 16:23:35 HST

In Vol 15, issue 40, Jim Wolper stated that it would be difficult to implement digital signatures into the IFF transponder system. The military has been doing this for many years now. There is an IFF mode in which there is an encrypted "code of the day" transmitted by the interregator set, to which only a properly keyed transponder will reply. In a very similar way, the military mode of TACAN can encrypt ident and radial information to deny use of our TACAN to an enemy. And of course, the military can encrypt Global Position System transmissions to deliberately degrade it's use by non military users.

So it's not that difficult, just expensive to implement.

ETC Mark A. Bowers, Naval Computer and Telecomm., Area Master Stn, Eastern Pacific, Wahiawa, Hawaii mbowers@nctsemh-epac.navy.mil n911@pnet16.cts.com

✓ phony air traffic controller (Pereira, RISKS-15.39)

Cameron Strom <syscrs@devetir.qld.gov.au> Wed, 26 Jan 1994 10:07:47 -40962758 (EST)

> an out-of-work janitor pleaded guilty to giving false radio commands > to pilots

On January 25, the Brisbane Courier-Mail reported the following:

A teenager with a \$70 radio in his bedroom intercepted air traffic control channels and told two airline pilots to abort landings. The 17-year-old air cadet, obsessed with planes, also gave false reports of planes in distress and falsely instructed other aircraft for two weeks in December last year. He had learnt how to intercept radio transmissions as a member of the air cadets and from his time in the air traffic control tower on work experience as a Year 10 student. The control tower had been aware that someone had been abusing the system in the area and had been on extreme alert to make sure the pilots received correct instructions.

The lad has pleaded guilty to prejudicing the safe operation of aircraft. He is undergoing psychiatric assessment, and will be sentenced on March 28.

Cameron Strom syscrs@devetir.qld.gov.au Brisbane, Queensland, Australia.

✓ re: Smart Cars and Highways (Kabay, RISKS-15.35)

Jerry Leichter <leichter@lrw.com> Sun, 23 Jan 94 22:37:38 EDT

In <u>RISKS-15.35</u>, Mich Kabay reports on a Washington Post newswire story about the Government spending on an Intelligent Vehicle and Highway System, which is intended to provide a variety of advances leading up to the dream of computer-controlled cars.

The article is sub-titled "Washington's Latest Billion Dollar Boondoggle", so we know right off how it will be slanted. The story is the flip side of the "sales job" articles one too often sees. Were the director of this program to write a press release, it would certainly discuss all the great potential, including the potential of parts of the system no one really has any idea how to build, and none of the problems. The Post article discusses all the problems, including all the problems of versions of the system no one would consider building, without considering any of the possible advantages. In fact, one can look through the article and construct a guide to "how to write an article about the RISKS of a newly proposed system". Thus:

1. Compare to a system everyone loves to hate - no matter how little it has to do with the issue at hand:

"Government spending on the little-known Intelligent Vehicle and Highway Systems (IVHS) program is expected to exceed \$40 billion over the next 20 years. (By comparison, in the first 10 years of the Strategic Defense Initiative, Washington spent \$30 billion.)"

A more relevant comparison might be to the expected outlay of money over the next ten years on, oh, repaving existing roads, upgrading bridges, and so on. Also, how much of this cost is for development, and how much for deployment? SDI was all development costs. Deployment of almost anything on the scale of the national highway system - even something as simple as traffic lights to help control entry at busy on-ramps - quickly runs into the billions.

2. Demand proof before anything at all can be done:

"claims of improved safety are unproven"

3. Assume a system model that is known not to be applicable:

"central computer failures could lead to massive accidents"

It's hard to imagine any reason for centralized control of such a system. Has anyone actually proposed this?

4. Demand that the system solves problems that are outside of its purview:

"proposed fuel savings from smoother driving could be lost through higher speeds"

"minor attention given to smart public transport, priorities for high-occupancy vehicles"

Even if this is true, so what? Fuel savings are a social good; so is higher speed commuting. A smart highway system would give society the ability to make tradeoffs between them, to any desired degree. In what way is this a negative?

Smart public transport - whatever that might mean - would be a social good if we could get people to use it, but the fact of the matter is that most of the population long ago "voted with their feet" in preferring cars - and not "high-occupancy vehicles" at that - to public transport. This project does not attempt to join the long list of failed efforts to convince people that they really would prefer to be on a bus or train; it attempts to provide a better implementation of the choice they've already made. Again, why is this a negative?

5. When in doubt, name some big companies that like the idea - that can always be relied upon to generate uproar:

"main proponent of scheme is IVHS America, supported by 500 organizations including IBM, AT&T, Rockwell, General Motors, Chrysler, Ford"

6. Always, always stress the dangers to people, but don't mention the hazards of existing systems.

"Participants in RISKS will shudder at the thought of testing computer programs design to control thousands of cars in lockstep at 200 kph. I wouldn't enjoy being part of the beta-test population."

"proponents concerned with limiting liability for failures"

"I find the concern with legal liability an alarming indication of where we're headed."

The current "human controlled" highway system kills, what, 50,000 people a year? It has no effective mechanism for keeping significant numbers of drunk, drugged, or otherwise incapable drivers from wreaking havoc. It has no

effective mechanism for getting drivers to respond rationally to such problems as inclement weather. Dealing with the ice on the roads here the last week or so isn't nearly as scary as dealing with the idiots who think that four-wheel-drive will magically allow them to steer and stop at high speed no matter how slick the roads are.

The legal liability issue grows right out of this: Under the current legal system, evidence that something is less risky than what it replaced is not considered relevant; all that's considered relevant is that the system that actually *is* in effect hasn't prevented some injury. The current driving system is tolerated because it spreads the legal risk. If a new system cut the risk 100-fold, so that only 500 people a year died because of system problems, virtually everyone would consider that an unalloyed good - but if the result were 500 successful, massive lawsuits against whoever created, installed, and ran the new system, it would quickly collapse.

7. Make the technical problems appear clearly insoluble:

"Participants in RISKS will shudder at the thought of testing computer programs design to control thousands of cars in lockstep at 200 kph. I wouldn't enjoy being part of the beta-test population."

"I wonder how much attention will be paid to deliberate or accidental interference?"

"How will partial or total breakdown of the control systems be handled? Car-to-car signalling?"

"Presumably information will be transmitted through radio-frequency modems. What will the unique identifiers be for each car. What happens if two cars have the same identifier?"

"What methods will be put into place to prevent spurious instructions from being accepted by car controllers?"

Sorry, but none of these strike me as particularly difficult problems. 200kph requires reaction times that are not a problem with even fairly stupid control systems. "Thousands of cars" are not a problem unless one visualizes a system that controls them all from a central location. In fact, traffic control is the ultimate distributed problem, since the automobiles involved are distributed all over the world. The short-term choices that an automobile controller must make involve information about at most a few tens of other automobiles. Sure, long-term planning of routes and such requires more global information, but this is not a safety issue, and is not time-critical.

It is easy to design "fail safe" modes for automobiles when there is some kind of system failure; all that's necessary is to gradually slow to a stop. In fact, this is something we handle rather poorly today - consider what happens when a front tire blows out in heavy, rapid traffic, or the repeated instances of multi-car collisions when visibility drops. Almost any reasonable system would be an improvement, and would probably save lives.

This also relates back to point 3, "Assume a system model that is known not

to be applicable". While the article didn't happen to address this point, complaints about the difficulty of creating such systems usually assume that the most advanced form (full computer control) will exist in parallel with the current system (full human control, pedestrians, bicyclists) on the same roads. That makes the system much, much harder - but why would we wish to build it that way? Highways today already assume limited access; why would we not designate some highways - or perhaps lanes of existing highways isolated by crash barriers - for computer controlled use only?

Really, I can't believe anyone is concerned about the difficulty of ensuring that every car has a unique identifier. If it bothers you, use a 512-bit id and have the car pick one randomly every time it is turned on. The chance of a clash should be comparable to the chance that all the molecules in the car's gasoline simultaneously happen to break apart in a spectacular fireball. It would also make it much harder to track a particular automobile. Then again, why does a car need a globally-unique identifier anyway unless you assume the model of a single, central controller?

That leaves the security issues, which are of course quite real and worthy of significant concern and careful design. But do they really look daunting enough to make the whole project clearly impossible? One important effect of almost any technology is that it increases the "leverage" an individual has. This "leverage" can be used for many purposes, some of them malignant. What's important are the tradeoffs.

As an interesting exercise, one can apply the seven techniques outlined above - there are undoubtedly others, like "argue that the system will disproportionately injure the poor" - to argue, early this century, that automobiles should not be developed to replace horses. For example:

2. Demand proof before anything at all can be done:

We know how reliable horses are. Can you prove that you can build a gas engine as reliable as a horse?

3. Assume a system model that is known not be be applicable:

It's one thing to keep supplies of hay and oats at home, but would you want everyone to keep a tank of gasoline at home to keep his car filled up? Think of the fire hazard!

5. When in doubt, name some big companies that like the idea - that can always be relied upon to generate uproar:

Actually, you can list some of the same companies....

And so on.

-- Jerry

Telescript risks

<blakley@vnet.IBM.COM>

Wed, 26 Jan 94 16:03:19 EST

I think the discussion of telescript risks here so far misses the two most important points:

- (1) It doesn't really matter whether telescript agents "directly manipulate the memory, file system, or other resources of the computers on which they execute"! If they're going to be useful as "agents", they're going to be authorized to use the interfaces of their host systems to do some amount of useful work. Presumably, since users don't want to administer authorization on a user-by-user basis when the potential user set is "everyone on the worldwide internet", either:
 - (a) The telescript agent on most machines is going to be a "somewhat privileged" or "highly privileged" trusted program, with access to a useful set of system services, utilities, and applications, or
 - (b) The telescript agent on most machines isn't going to have access to much useful functionality.
 - If (b) turns out to be the default, then our worries are limited. The worst permutation of (a) is that everyone installs the telescript agent on his workstation as the equivalent of a "setuid root" program, which allows it to do anything it wants..... Then it's just a matter of the "bad guy" writing a program in the interpreted language which invokes the desired functions on the remote machine.....

The bad guy will *of course* be able to do this -- the whole *point* of Telescript is to make it easy to write programs which can invoke arbitrary functions on remote machines.

The point here is that regardless of how much *mechanism* support is built into Telescript, the real problem is the complexity of administering authorization policy in a network in which:

- (a) There is no central administrative authority (i.e. most machines have their own unique security administrators), and
- (b) The people generating requests (i.e. releasing telescript programs into the network) have no idea where those requests are going to end up.
- (2) But of course the really bad problem which isn't addressed by any authentication or access control mechanism is the problem of emergent behavior in the network. Nobody knows what the dynamics of a network filled with end-user-written, self-routing "semi-intelligent" agents is. My bet is that IP storms are nothing compared with the weather we're going to get when substantial numbers of these agents start roving around....

Usual disclaimers apply along with the following unusual one: The author is G.R. (Bob) Blakley III (Security Architect, IBM LAN Systems, Austin TX), NOT G.R. (Bob) Blakley, Jr. (Mathematician & Cryptographer, Texas A&M University, Bryan TX)! Phone (512)838-8133 t/l 678-8133, FAX 838-1040

Re: Can SETI signals bear viruses?

Andrew Klossner <andrew@frip.wv.tek.com> Wed, 26 Jan 94 12:31:01 PST

Some serious naivete here ...

"You don't need to worry about spreading viruses if you transfer data disks (say, word processing or spreadsheet files) between computers."

It's not so. People can, and do, spread viruses by carrying Macintosh data disks from one machine to another. Spreading viruses via PC data disks is a bit harder, but does happen.

"Well, hopefully if it comes to that one of our Heroic Scientists will have the presence of mind to read the bloody code before they run it!"

I have seen malicious programs whose source was written in such a way that a careful read wouldn't necessarily betray its malicious character.

-=- Andrew Klossner (andrew@frip.wv.tek.com)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 42

Friday 28 January 1994

Contents

- CFP '94: THE FOURTH CONFERENCE ON COMPUTERS, FREEDOM AND PRIVACY
- Info on RISKS (comp.risks)

✓ CFP'94 (fwd)

"Lance J. Hoffman" <hoffman@seas.gwu.edu> Sun, 23 Jan 1994 10:44:40 -0500 (EST)

CFP '94

THE FOURTH CONFERENCE ON COMPUTERS, FREEDOM AND PRIVACY MARCH 23-26, 1994 CHICAGO PALMER HOUSE HILTON

"CYBERSPACE SUPERHIGHWAYS: ACCESS, ETHICS and CONTROL"

SPONSORS

ASSOCIATION FOR COMPUTING MACHINERY

SPECIAL INTERESTS GROUPS ON:

COMMUNICATIONS (SIGCOMM)

COMPUTERS AND SOCIETY (SIGCAS)

SECURITY, AUDIT AND CONTROL (SIGSAC)

JOHN MARSHALL LAW SCHOOL, CENTER FOR INFORMATICS LAW

PATRONS & SUPPORTERS (as of 15 December 1994)

AMERICAN EXPRESS CORP.

BAKER & McKENZIE

EQUIFAX, INC

LEGAL TRUSTEES, JERSEY, LTD. (UK)

MOTOROLA, INC

NATIONAL SCIENCE FOUNDATION (PENDING)

WIRED MAGAZINE

COOPERATING ORGANIZATIONS

AMERICAN BAR ASSOCIATION SECTION OF
SCIENCE AND TECHNOLOGY

AMERICAN CIVIL LIBERTIES UNION
COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY
ELECTRONIC FRONTIER FOUNDATION
GEORGE WASHINGTON UNIVERSITY INSTITUTE for COMPUTER and
TELECOMMUNICATIONS POLICY
IEEE COMPUTER SOCIETY
IEEE-USA COMMITTEE ON COMMUNICATIONS
AND INFORMATION POLICY
LIBRARY AND INFORMATION TECHNOLOGY ASSOCIATION
PRIVACY INTERNATIONAL
U.S. PRIVACY COUNCIL

UNITED AIRLINES IS THE OFFICIAL AIRLINE FOR CFP'94

Fourth Conference on Computers, Freedom and Privacy Chicago, II., March 23 - 26, 1994

CFP'94, "Cyberspace Superhighways: Access, Ethics and Control"

General Chair

George B. Trubow, Center for Informatics Law, John Marshall Law School

Executive Committee

George B. Trubow, Chair, CFP'94 Lance J. Hoffman, George Washington University, Chair, CFP'92 Bruce Koball, San Francisco, CA, Chair, CFP'93

Conference Treasurer

Robert Ashenhurst, University of Chicago

Special Promotions

Patric Hedlund, Sweet Pea Productions

Alan Whaley, The WELL, San Francisco

Manager, Volunteers and Conference Office Judi Clark, ManyMedia, Palo Alto

Chair, Student Writing Competition Gene Spafford, Purdue University

Co-Chairs, Student Scholarship Program
John McMullen, Marist College

James Thompson, Northern Illinois University

Program Committee

David Banisar, Computer Professsionals for Social Responsibility Jerry Berman, Electronic Frontier Foundation Robert Belair, Mullenholz and Brimsek
Roger Clarke, Australian National Univesity
Mike Godwin, Electronic Frontier Foundation
Mark Hellmann, Pattishall, McAuliffe
Linda Knutson, Library & Information Technology Association
Dennis McKenna, Government Technology Magazine
Michael Mensik, Baker & McKenzie
Ron Plesser, Piper and Marbury
Priscilla Regan, George Mason University
Lance Rose, LOL Productions
Marc Rotenberg, Computer Professionals for Social Responsibility
Robert Ellis Smith, Privacy Journal
James Thompson, Northern Illinois University
Alan F. Westin, Columbia University

Conference Administration by John Marshall Law School: Arrangements Director, RoseMarie Knight Publicity & Publications, John McNamara Financial Officer, James Kreminski Program Coordinator, Gary Gassman

CYBERSPACE SUPERHIGHWAYS: ACCESS, ETHICS and CONTROL

Cyberspace, Information Superhighway, National Information Infrastructure, Open Platforms, Computer and Communications Revolution, Electronic Networks, Digital Data Bases and Information Society are words and phrases common to the rhetoric of our modern era. The relationships between and among individuals, society, nations, government entities and business organizations are in constant flux as new stresses and alliances change the old "rules of the game." Today's challenges are to define what is the "game," who owns the "franchises," who can play, what are the rules and who calls the shots. Information and communications technology raise new issues for freedom and privacy in this new era. Such questions are on the agenda as the participants in CFP'94 consider the alternatives and seek some solutions. Come, join in the dialogue that will help to shape the world's future!

PRE-CONFERENCE TUTORIALS

On Wednesday March 23, the day before the formal conference begins, CFP '94 is offering a number of in-depth tutorials covering a wide variety of subjects on five parallel tracks. These presentations will be interesting, educational, thought-provoking and often controversial. The tutorials are available at a nominal additional registration cost.

CONFERENCE NEWSPAPER

On each of the three days of the conference, a daily newspaper will appear to highlight what has transpired and announce important coming events. The staff of "The Decisive Utterance," The John Marshall Law School's student newspaper, is providing this service.

CONFERENCE RECEPTION AND TECHNOLOGY DISPLAY

On Wednesday evening, from 6:00 p.m. - 9:00 p.m., you are invited to meet new and old friends and colleagues at an opening reception at the John Marshall Law School from 6:00 p.m.-9:00 p.m. The School is only two blocks from the conference hotel. A state-of-the-art computer lab will be used to demonstrate high-tech applications in academia and registrants will be invited to take part.

SINGLE-TRACK MAIN PROGRAM

The technological revolution that is driving change in our society has many facets and we are often unaware of the way they all fit together, especially those parts that lie outside one's own daily experience. An important goal of CFP '94 is to bring together individuals from disparate disciplines and backgrounds and engage them in a balanced discussion of CFP issues. To this end our main program, starting on Thursday, March 24, is on a single track enabling registrants to attend all sessions. The concurrent Birds-of-a-Feather meetings Thursday after 9:15 p.m. are exceptions.

BIRDS OF A FEATHER SESSIONS (BoF)

CFP '94 will provide a limited number of meeting rooms to interested individuals for informal "Birds of a Feather" sessions after the formal program Thursday, from 9:15 p.m. - 11:15 p.m. These sessions will provide an opportunity for special-interest discussions. For further information or to request a BoF contact CFP '94 Program Coordinator, Gary Gassman, at the John Marshall Law School (6gassman@jmls.edu)

MUSEUM OF SCIENCE AND INDUSTRY GALA

Registrants are invited to a very special reception and buffet at Chicago's famed Museum of Science and Industry where they also will be treated to a private showing and demonstration of the MSI's newly-opened Communications and Imaging Exhibits. These multi-million dollar presentations occupy 15,000 sq.ft. of museum space and required three years to develop. "Communications" is a panoramic display of how technology has transformed our lives by dissolving distance and and making connections; visitors can even enter the unreal world of virtual reality. "Imaging" is a mindboggling journey through modern applications of imaging technology. Visitors can even play the role of brain surgeon, using radiosurgery made possible by 3-D imaging, or explore imaging in forensic science by using MRI, fingerprint enhancement, face aging and other modern technologies to solve a crime!

REGISTRATION WILL BE LIMITED

CFP '94 registration will be limited to 550 attendees, so we advise you to register early to assure admission and to take advantage of the early registration discounts.

MEALS AND RECEPTIONS

A key component of the CFP conferences has been the interaction between the diverse communities that constitute our audience. To promote this interaction CFP '94 provides three luncheons, three receptions and three evening meals

with the price of registration.

EFF PIONEER AWARDS

All conference attendees are invited to the EFF Pioneer Awards Reception sponsored by the Electronic Frontier Foundation on Thursday evening. These, the third annual EFF Pioneer Awards, will be given to individuals and organizations that have made distinguished contributions to the human and technological realms touched by computer-based communications.

CONFERENCE BUSINESS OFFICE

The Conference business and registration office will be open from 8:00 a.m. until 9:00 p.m. on Wednsday thru Friday, and until 6:00 p.m. on Saturday, for registration and general information.

NOTE: The following program content and schedule is subject to change. The Information Superhighway is a fast track!

Wednesday, March 23, 1994 Pre-Conference Tutorials

9:00 a.m. - noon

Cyberspace Law for Non-Lawyers
This tutorial presents an outline of the law for laymen,
dealing with Constitutional and legal issues that confront
those concerned with privacy, crime, and freedom of expression
in cyberspace. There will be summaries of recent cases,

Mike Godwin, Online Counsel, EFF

legislative proposals and government activities.

Rules of the Road for Network Travelers. (CLE Credit Approved) The information superhighway presents a variety of rights and risks. Learn about the legal issues of computer networks, services and bulletin boards, including on-line property rights; protecting personal privacy and business information; electronic publishing and multimedia rights; viruses, adult materials and other no-nos.

Lance Rose, Attorney and Author of "Syslaw."

Get Mad, Get Motivated, Get Moving!

The focus of this panel is on citizen action for privacy protection: how to reach and organize constituents; support legislation or other privacy protection measures; conduct public education activities; use the technology in program activities, etc.

Robert Ellis Smith, Privacy Journal

Exploring Internet: A Guided Tour
This tutorial gives participants a practical introduction to
the most popular and powerful applications available via the
world's largest computer network, the Internet. There will be

hands-on demonstrations of communications tools such as email, conferencing, Internet Relay Chat and resource discover, and navigations aids such as Gopher, WAIS, Archie and World Wide Web. Extensive documentation will be provided.

Mark Graham, Pandora Systems

Using the Freedom of Information Act
The Federal FOIA is the principal focus of this tutorial
though some attention is given to the use of state FOIAs.
The session will cover procedures for making requests,
identifying the information desired, differences between
electronic and hard copy responses, and the appeals process
within agencies and the courts.
David Sobel, Counsel, Computer Professional for Social
Responsibility

2:00 p.m. - 5:00 p.m.

Cryptography: What, and How?

Data encryption is in the cyberspace limelight as perhaps the only technique to ensure digital privacy and security; it is also the subject of sharp debate regarding control of the development and use of the technology. This tutorial will display what encryption is, how it works, and some of the options for its use. Computer animations and graphic displays will be used to help make cryptography comprehensible; the audience will engage in some hands-on encryption exercises.

Mark Hellmann, Pattishall, McAuliffe et.al, Chicago

Electronic Detectives: Critical Issues for Public and Private Investigators.

Both governmental and private sector investigators have unprecedented access to "open" sources that were practically inaccessible a few years ago. This information environment poses opportunities and risks that will be the focus of this program. Investigative techniques via networks will be demonstrated and the legal, ethical and practical issues will be explored. Actual case-studies will be utilized. Michael Moran, CCO; Michael Robertson, CFE

Hi-Tech Intellectual Property Law Primer (CLE Credit Approved)
This panel will cover the special problems in patent,
copyright and tradmark law engendered by computers and digital
technology, with attention to the impact of recent cases. The
differences in European protection will be surveyed as well as
technology export restrictions.

Raymond Nimmer, University of Texas Law School Leslie A. Bertagnolli, Baker & McKenzie, Chicago

Transactional Data Analyses: Making FOI Access Useful Electronic communication, coupled with federal and state Freedom of Information Acts, has made a great deal of data available to the public regarding the activities and policies of government enforcement and regulatory agencies. Knowing

how to evaluate and use this information is critical to understanding and demonstrating what the data really means. The Transactional Records Access Clearinghouse (TRAC) of Syracuse University uses its various knowledge-bases to demonstrate the power of transactional data. Colorgraphics and analytic techniques are combined in demonstrations of how otherwise drab statistics can be displayed dramatically to aid in policy analyses and advocacy.

David Burnham, former New York Times Investigative Reporter Susan Long, Co-director, TRAC, SUNY-Syracuse

Election Fraud and Modern Technology
There has been increasing attention, in the U.S. and abroad, to the use of modern technology in the electoral process.
Buying votes, stealing votes, changing votes -- whether in the environment of punch-cards or fully automated voting machines -- is the subject of this tutorial. Mock elections will be staged in which the participants have roles in planning to perpetrate as well as prevent vote fraud. Voter registration, phone-based voting, cryptography and verification are among the strategies and technologies to be considered.
Russel L. Brand, Reasoning Systems.

SPECIAL EVENTS ON WEDNESDAY, Mar. 23:

Noon - 4:00 p.m., Privacy International Business Meeting
This meeting, at the John Marshall Law School, begins with a
buffet luncheon. Non-members interested in learning about
P.I. and the Illinois Privacy Council are invited to be guests
for lunch and a briefing. Guest space will be limited so
attendance on a "first come" basis MUST be confirmed by
March 8, 1994.

6:00 p.m. - 9:00 p.m. Conference Reception

All CFP registrants are invited to a reception and open house demonstrating the John Marshall Law School's recently opened computer lab. This also is an opportunity to "network" the old-fashioned way, meeting old friends and making new ones while enjoying the reception and buffet. This state-of-the-art facility will display information and communications technology being used in the educational environment. Guests also may participate in hands-on demonstrations of the technology under the tutelage of JMLS faculty and staff.

9:15 p.m. - 11:15 p.m. "CFP SOAPBOX SQUARE"

On Wednesday, March 23, from 9:15 p.m. to 11:15 p.m., "CFP Soapbox Square" will be open. This is a chance for those who have something to say publicly to say it and to hear response from others! Those interested in making a brief statement (3 minutes) at this meeting must file their request and describe their topics by 5:00 p.m. on Wednesday. Discussion time for various topics will be allocated based upon the number of topics and the number who

have asked to speak. Requests to speak can be made at the time of pre-registration or at the conference site.

Thursday, March 24, 1994

8:30 a.m., CFP'94 Official Opening

Welcome to the Conference: George B. Trubow, General Chair Welcome to Chicago: Hon. Richard M. Daley, Mayor (Invited)

9:00 a.m. Keynote Address: Mr. John Podesta, Assistant to the President, Washington, D.C.

10:00 a.m. Break

10:30 a.m. The Information Superhighway: Politics and the Public Internet

The Administration and Congress propose policies that will lead to a digital multimedia highway. How can the road be built at affordable cost while serving the public interest and our constitutional values?

Chair: Jerry Berman, Electronic Frontier Foundation

12:00 p.m. Lunch

Speaker: U.S. Senator Paul Simon (Invited)

1:30 p.m. Is It Time for a U.S. Data Protection Agency?

Beginning with the Privacy Act of 1974, proposals to establish an oversight body for data protection have been offered but not adopted; another proposal is currently pending in Congress. Against a background of almost twenty years experience under the Privacy Act, the panel will consider whether the current political, economic and technological mileau favors establishment of a data protection agency. Chair: Priscilla M. Regan, George Mason University

2:45 p.m. Break

3:00 p.m. "Owning and Operating the NII: Who, How, When?"

The National Information Infrastructure is an important initiative for the present Administration. This panel will explore policy and technical issues such as equity and access, connectivity and standards, funding and regulation, privacy and security, ownership and operation.

Chair: Marc Rotenberg, Computer Professionals for Social

4:15 p.m. Break

4:30 p.m. Data Encryption: Who Holds The Keys?

Recent attempts, led by federal law enforcment agencies, to control the development and dissemination of strong cyptography programs has engendered considerable discussion

and disagreement. The interests of law enforcement agencies may conflict with the need for data security and personal privacy demanded by users of electronic networks. This panel will evaluate proposals to deal with the question. Moderator: Willis Ware, Rand Corporation

5:30 p.m. Adjourn

6:00 p.m. EFF Awards Reception

Once again, the Electronic Frontier Foundation hosts a reception prior to its annual Pioneer Awards presentation. All CFP attendees are invited to enjoy the recepiton and congratulate the new honorees.

7:00 p.m. Conference Banquet (Speaker to be announced)

9:15 - 11:15 p.m. "Birds-of-a-Feather" sessions run concurrently.

Friday, March 25, 1994.

8:30 a.m. Keynote: David Flaherty, Data Protection Commissioner, Victoria, British Columbia

9:15 a.m. Health Information Policy

The Clinton Health Reform Plan, and variations on that theme, stress the use of information technology to help the efficiency and effectiveness of health care. Expert consultation, improved service delivery through new technology, and improvements in the processing of health insurance claims bring promise of cost cuts as well as the possibilities of threats to personal privacy. This panel of experts will form the "CFP Group" to explore these promises and threats.

Chair: Robert R. Belair, Mullenholz & Brimsek, Wash., D.C.

10:30 a.m. Break

10:45 a.m. Can Market Mechanisms Protect Consumer Privacy?

When does protection of consumer privacy require legal standards and government regulation and when can bargains and agreements in the market suffice? What role do new technological options for individuals and organizations play in facilitating private choice and market transactions? Is "ownership" of personal information a useful concept or a dead end for privacy protection in an information age?

Chair: Dr. Alan F. Westin, Columbia University

Noon Lunch, Speaker: Philip Zimmerman, PGP

1:30 p.m. Creating an Ethical Community in Cyberspace

The fundamental ethical questions posed by the "settlement" of cyberspace are not new. What is new is that the relationship

between behavior and the ethical conceptions by which we judge behavior shift and become more ambiguous and vague. This sessions examines the ethical dilemmas brought about by the "colonization" of cyberspace that must be resolved to establish and maintain a stable, humane environment. Chair: Prof. James Thomas, Northern Ilinois University

2:45 p.m. Break

3:00 p.m. Standards for Certifying Computer Professionals
The subject of licensing of computer professionals is
receiving increased attention by professional organizations
and by state legislatures. Both the ACM and IEEE have
proposals under study, and perhaps a half-dozen states are
considering licensing bills. This panel will consider the
pros and cons and suggest some standards for certification.
Chair: Donald Gotterbarn, East Tennessee State Univ.

4:15 p.m. Break

4:30 p.m. Hackers and Crackers: Using and Abusing the Networks
This session will explore issues surrounding the "fringe" of
network use. What can and should be exchanged? Who will
monitor "appropriate" use? What's the current difference, if
any, between "hacker" and "cracker"? What should be expected
and accepted regarding the role of law enforcement agencies?

5:30 p.m. Adjourn

5:45 p.m. Buses begin departing for the Chicago Museum of Science and Industry for a private reception and demonstration at the Communications and Imaging exhibits.

9:00 p.m. Buses begin departing for return to the Palmer House and Chicago's "Loop."

Saturday, March 26, 1994

9:00 a.m. The Role of Libraries on the Information Superhighway As the information landscape changes dramatically the historic role of libraries as the "information commons" is challenged. How will the Carnegie ideal of free, public access be implemented by the library community? Should it be? This panel will consider policy for an information network in the public interest.

Moderator: Tamara J. Miller, President, Library and Information Technology Association

10:15 a.m. Break

10:30 a.m. International Governance of Cyberspace: New Wine in Old Bottles -- Or Is It Time For New Bottles?
Much discussion transpires between members of the Economic Community, the O.E.C.D., the Council of Europe, and the United

States, regarding data protection, intellectual property rights, transborder data flow, the mediation of disputes, etc. This panel will consider whether existing mechanisms can solve the problems or a new structure for the governance of cyberspace is needed.

Chair: Ronald L. Plesser, Piper and Marbury

Noon: Lunch

Speaker: Simon Davies, Director General, Privacy

International

1:30 p.m. The Electronic Republic: Delivery of Government Services over the Information Superhighway

State and local governments use computer networks to deliver a wide range of services and information to the public; electronic "kiosks" are moving to "government by ATM." How will this interaction between government and the people affect the process of American government in the future?

Chair: Dennis McKenna, Publisher, "Government Technology."

2:45 p.m. Break

3:00 p.m. Education and NREN, K - 12

Internetworking is a very new technology being rapidly deployed to conventional classrooms, a very old technology. The panel will explore the clash of contradictory assumptions embedded within these systems -- a clash which has profound implications for the future of both the network and the classrooom.

Chair: Steven Hodas, NASA NREN Project

4:00 Break

4:15 p.m. Guarding the Digital Persona

After this panel has established the threats to personal privacy from individual profiling and target marketing, and a regime to legally recognize and protect an "electronic personality" is put forth, Bruce Sterling will offer to explain why much of that worry is misdirected!

Chair: Roger Clarke, Australian National University

5:30 p.m. Adjournment

Featured Speakers Confirmed as of 12/15/93

Philip Agre, Dept. of Sociology, U. of Cal., San Diego
David Banisar, Computer Professional for Social Responsibility
Robert R. Belair, Mullenholz & Brimsek, Washington, D.C.
Jerry Berman, Executive Director, Electronic Frontier Foundation
Leslie A. Bertagnolli, Baker & McKenzie, Chicago
Andrew Blau, The Benton Foundation, Washington, D.C.
Dr. Herbert Burkett, GMD, Koln, Germany

Jeffrey Chester, Director, Center for Media Education Roger Clarke, College of Commerce, Australian National University Ellen Craig, Commissioner, Illinois Commerce Commission Simon Davies, Director General, Privacy International, London David Flaherty, Data Commissioner, British Columbia Oscar H. Gandy, Media Studies Center, Columbia University Donald Gotterbarn, East Tennessee State University Allan Hammond, New York University Law School Steven Hodas, NASA NREN Project, Washington, D.C. David Johnson, Wilmer, Cutler & Pickering, Washington Steven Kolodney, Dir., Information Technology, State of California Curtis Kurnow, Landels, Ripley & Diamond, San Francisco Kenneth Laudon, School of Information Systems, New York University Lee Ledbetter, HDX Jay Lemke, School of Education, City University of New York Duncan MacDonald, V.P. & Gen. Couns., Citicorp Credit Services

Shirley Marshall, Public Sector Marketing, IBM Dennis McKenna, Publisher, Government Technology Magazine Michael Mensik, Baker & McKenzie, Chicago Raymond Nimmer, University of Texas Eli Noam, Columbia University School of Business Michael North, President, North Communications Ronald L. Plesser, Piper and Marbury, Washington, D.C. Marc Rotenberg, Computer Professionals for Social Responsibility Rohan Samarajiva, Department of Communication, Ohio State Univ. David Sobel, Computer Professionals for Social Responsibility Bruce Sterling, Sci-Fi Writer and Journalist, Austin, Texas Connie Stout, Texas Education Network James Thomas, Department of Sociology, Northern Illinois University Greg Tucker, Head of the Business School, Monash Univ., Australia Bruce Umbaugh, Old Dominion University Patricia Valey, Acting Director, Office of Consumer Affairs Maarten van Swaay, Dept. of Computer Science, Kansas State U. Daniel Weitzner, Sr. Staff Counsel, Electronic Frontier Foundation Alan Westin, Columbia University

REGISTRATION

Register for the conference by returning the Registration Form along with the appropriate payment. The registration fee includes conference materials, three luncheons (Thursday, Friday and Saturday), a reception, open house and buffet (Wednesday), a reception and banquet (Thursday), and a gala reception and buffet at the Museum of Science and Industry. Payment must accompany registration.

REGISTRATION FEES

If paid by: 7 February 8 March On Site Early Regular Late

Christine Zahorik, Staff, Senate Committee on

Conference Fees \$315 \$370 \$420 Tutorial Fees \$145 \$175 \$210 Conf. & Tutorial \$460 \$545 \$630 Save by Registering Early!

FP '94 SCHOLARSHIPS

The Fourth Conference on Computers, Freedom and Privacy (CFP '94) will provide a limited number of full registration scholarships for students and other interested individuals. These scholarships will cover the full costs of registration, including luncheons, two banquets, and all conference materials. Scholarship recipients will be responsible for their own lodging and travel expenses. Persons wishing to apply for one of these fully-paid registrations should contact CFP '94 Scholarship Chair:

John F. McMullen
CFP '94 Scholarship Committee
Perry Street
Jefferson Valley, NY 10535
Phone: (914) 245-2734 or email mcmullen@mindvox.phantom.com

HOTEL ACCOMMODATIONS

CFP'94 will be held at the Palmer House Hilton, a venerable Chicago landmark in the "Loop." This spacious and comfortable facility is easily accessible from the O'Hare International and Chicago Midway airports, and is only 2 blocks from The John Marshall Law School. Special conference rates of \$99/night, single or multiple occupancy, are available. Our room block is guaranteed only until March 1, 1994, so we urge you to make your reservations as early as possible. When calling for reservations, please be sure to mention CFP'94 to obtain the conference rate.

Hotel Reservations: Palmer House Hilton, 17 E. Monroe, Chicago, Il., 60603. Tel: 312-726-7500; 1-800-HILTONS; Fax, 312-263-2556

REFUND POLICY

Refund requests received in writing by March 8, 1994 will be honored. A \$50 cancellation fee will be applied. No refunds will be made after this date; however, registrants may designate a substitute.

OFFICIAL AIRLINE

CFP'94 is proud to have United Airlines -- Chicago's Own -- as our own exclusive official airline! United will give our conferees a 5% discount off any published United or United Express airfare, including First Class, or 10% off the new BUA fare when purchased at least a week in advance of travel. Call toll-free 1-800-521-4041 to make reservations and be sure to give our CFP'94 ID Number: 541QI.

REGISTRATION

NAME (Please Print) TITLE **AFFILIATION** MAILING ADDRESS CITY, STATE, ZIP **TELEPHONE** E-MAIL PRIVACY LOCKS: We will not sell, rent. loan, exchange or use this information for any purpose other than official Computers, Freedom and Privacy Conference activities. A printed roster containing this information will be distrusted at the conference. Please indicate if you wish information to be excluded from the roster: () Print only name, affiliation and phone no. () Print name only () Omit my name from the roster () I would like to attend the Privacy International luncheon and briefing at noon on Wednesday, March 23. (Your attendance as a guest of P.I. and the Illinois Privacy Council MUST be confirmed by March 8, and is on a "first come" basis.) "CFP Soapbox Square" () I would like to make a formal statement (3 mins.) during "CFP Soapbox Square" to be held from 9:15 p.m. - 11:15 p.m. on March 23. My topic: () I plan to attend "Soapbox Square" but do not wish to make a prepared statement, though I may join in the discussion. **REGISTRATION FEES** If paid by: On Site 7 February 8 March Early Regular Late \$370 Conference Fees \$315 \$420 **Tutorial Fees** \$145 \$175 \$210 Conf. & Tutorial \$460 \$630 \$545 Note: If you have registered for the Tutorials, please select one from each group: 9:00 A.M. - 12:00 NOON () Cyberspace Law for Non-Lawyers () Rules of the Road for Network Travelers (CLE Credit)

() Citizen Action: Get Mad, Met Motivated, Get Moving!

() Exploring Internet: A Guided Tour () Using FOIA			
2:00 P.M 5:00 P.M.			
() Cryptography: What, and How?			
() Introduction to Hi-Tech Law (CLE Credit)			
() TRAC: Evaluative Data Analysis			
() The Electronic Detective" Online			
Investigations			
() Electoral Fraud			
MENTS TOTAL AMOUNT			

PAYI

Please indicated method of payment:

- () Check (payable to JMLS-CFP '94)
- () VISA
- () MasterCard

Credit Card #

Expiration Date

Name on Card

Signature

"Computers, Freedom & Privacy '94", The John Marshall Law School 315 South Plymouth Court, Chicago, Illinois 60604 e-mail = cfp94@jmls.edu voice = 312/987-1419

General Chair: **Conference Coordinator:** George B. Trubow Gary L. Gassman

e-mail = 7trubow@jmls.edu e-mail = 6gassman@jmls.edu



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 43

Saturday 30 January 1994

Contents

Where has your Floating Point floated to?

Dave Wortman

Canadian TeleSat Anik E-2 Down

Colin Perkel

Luis Fernandes

Re: Lightning on the Ethernet

Jon Peatfield

Re: Spontaneous recovery from "NOMAIL" setting

Al Stangenberger

Ron Ragsdale

Peter M. Weiss

Re: Verify your backups

Rob Horn

Dick Hamlet

Crypto policy report available online

Lance J. Hoffman

1994 IEEE Symposium on Research in Security and Privacy

Catherine A. Meadows

Info on RISKS (comp.risks)

Where has your Floating Point floated to?

Dave Wortman <dw@pdp1.sys.toronto.edu> Thu, 27 Jan 1994 12:27:02 -0500

For those of you who think floating point computation is easy, I recommend as an antidote:

Jean-Francois Colonna, The Subjectivity of Computers Communications of the ACM, v.36,n.8, August 1993

where he demonstrates the five **algebraically equivalent** formulae for computing $x[n] = (R+1)x[n-1] - Rx[n-1]^{**2}$ produce wildly different results even for fairly innocuous values of R and x[0].

Canadian TeleSat Anik E-2 Down (A.Wexelblat, RISKS-15.41)

Colin Perkel <colin.perkel@guildnet.org> Sat, 29 Jan 1994 18:17:30 -0500

The trouble began with Telesat's Anik E-1 going down. This caused major problems for the Canadian Press news agency and its affiliate Broadcast News, as well as several other organizations. One casualty was telephone service to the North.

After eight hours, Anik E-1 was brought back on line but within minutes, Anik E-2, the country's main broadcast satellite, also went on the fritz.

This knocked out TV transmission of several specialty channels, including CBC Newsworld (24 hour news service), to all areas where there are no fibre optics. These channels were switched to other satellites and most services were restored in a couple of days.

Anik E-2 cost about \$350 million to send up, and is not insured. Montreal-based Telesat says it is working on a possible rescue plan that could take months. For the time being, the satellite is expensive space junk.

The coincidence of the two failures sparked all kinds of speculation: that either someone at Telesat screwed up big time, or a disgruntled grunt (perhaps from sweeping layoffs recently) sabotaged the bird. There was also a suggestion Telesat engineers damaged E-2 while trying to get E-1 back in business. These scenarios have all been denied. The official line is that an unusually strong magnetic storm did the damage (although other satellites nearby were not affected).

★ Re: Canada loses satellite-- more info (A.Wexelblat, RISKS-15.41)

luis fernandes <elf@ee.ryerson.ca> Fri, 28 Jan 94 16:58:36 EST

The Toronto Star, January 27, 1994, p.D2.

OTTAWA (Special [Southam News]) -- Canada's main broadcast satellite may resume operating within three months, the president of Telesat Canada says. "It is my firm belief we will restore service", Larry Boisvert told reporters Tuesday at the company's suburban Ottawa headquarters. Technicians are trying to use the satellite's 10 thrusters, normally used only to control major variations in position, to restore the fine aim needed to offer full service.

As of yesterday morning, Telesat had restored all service lost last week except for channels used by two broadcast channels and eight channels used by Telesat's telephone company owners. The company is also unable to offer television news services live feeds for mobile crews. The current troubles mean the company will again lose money in 1994, Boisvert said.

Meanwhile, Telesat technicians say there is no way to repair the damage inflicted last Thursday on the \$286 million satellite's stabilization system by a space energy storm. The technicians are, however, trying to devise a novel method of keeping the Anik E-2's antennae pointed at earth, working with

the device's U.S.-based subcontractor.

The damaged satellite is not insured.

[Further reports were also noted by John Oram <oramy92@halcyon.com> Jonathan_Welch <JHWELCH@ecs.umass.edu>, herdman@gov.on.ca (Andrew P. Herdman), and erling@wm.estec.esa.nl (Erling Kristiansen). Sorry I could not run them all... PGN]

Re: Lightning on the Ethernet (Eddy, RISKS-15.41)

Jon Peatfield <J.S.Peatfield@amtp.cam.ac.uk> Sat, 29 Jan 94 03:56 GMT

This isn't the story as it usually is told. ;-)

True the two maths departments (applied maths and theoretical physics (DAMTP) and pure maths and mathematical statistics (DPMMS)) are next door to each other, and that DAMTP was involved in this, but DPMMS wasn't (to the best of my knowledge.) Nice rumour though, blame the pure maths dept.

When I joined DAMTP in September '91 it was the week following the largest thunderstorm in several years. Sure enough many machines had got fried by the storm. Mainly it was serial lines which had died, though a few other bits and pieces had also been zapped.

We did however see a large number of giant packet storms on one of our first floor segments afterwards. A number of people were involved in the tracking down of the fault, as it didn't seem to be any of the machines on the network. After a while the link going outside and over into manufacturing Engineering (Eng-Div E), was found and it turned out that the fault was a PC at the far end of this wire which had lost all sense and was filling the net with garbage. The network was terminated before the window in DAMTP and we were happy.

Later checks showed that this had been installed temporarily (several years before) as building work was expected to disrupt the area where fibre links were laid but had never actually happened.

We had the now much shorter segment on the first floor TDR'd and found it was over a 100M over max length. How long it was when it ran half way round Eng-Div E is unknown.

Much later when searching for a fault on the ground floor we found another cable going out of a window, and cut it back/terminated it. Noone complained so we don't know where it had gone in the past.

Before anyone points out just how bad our network is, let me say "WE KNOW" The ethernet in this building was installed by someone who didn't know what they were doing. They worked for the UCS and we can't get funds to replace it. We

had no records of where cables go, nor their lengths. As time passes we are replacing/rewiring sections piecemeal. As I stare at the 2 30M coils of coax on the wall behind my desk which stop my feet getting tangled in the ethernet I wonder how many other networks like this one there are.

All links between DAMTP and DPMMS are done with fibre, and always have been. DAMTP and DPMMS are MAC level connected so there is/was no need for other links. Indeed at the time of the incident DAMTP and DPMMS shared at least 2 machines (though no longer.)

It isn't clear that unix-support had anything to do with this, other than they got told the story like everyone else who visits us.

The risks are obvious, never believe anything that unix-support tells you!

Jon Peatfield, Computer Officer, the DAMTP, University of Cambridge Telephone: (+44 223) 3-37852 Mail: J.S.Peatfield@amtp.cam.ac.uk

★ Re: Spontaneous recovery from "NOMAIL" setting

"Al Stangenberger" <forags@nature.berkeley.edu> Fri, 21 Jan 94 16:46:18 PST

Something like this happened recently on ECOLOG-L (sci.bio.ecology on Internet). I forget the specifics, but basically a mailed-in submission somehow triggered a flood of duplicate messages being sent out. In order to stop the replication the list owner set everybody's status to NOMAIL but there was no record of which users were already in NOMAIL status thus there was no way to reverse the process once the error was fixed except by setting everybody back to MAIL status.

I don't know if this was the listserver in question, but am cc-ing to the list owner who might be able to explain it more fully.

Al Stangenberger, Dept. of Env. Sci., Policy, & Mgt., 145 Mulford Hall - Univ. of Calif., Berkeley, CA 94720 (510) 642-4424 forags@nature.berkeley.edu

✓ Spontaneous recovery from "NOMAIL" setting?

Ron Ragsdale <R_RAGSDALE@oise.on.ca> Fri, 21 Jan 1994 15:13:39 -0500 (EST)

Setting "NOMAIL" to leave a LISTSERV keeps open the option of an easy return, but it may also lead to an unexpectedly full emailbox. Early in January, I began receiving regular messages from a LIST that I had set to NOMAIL in 1991; the LIST owner told me I was set to NOMAIL, but messages only/stopped when I sent an UNSUBSCRIBE message. Earlier this week (JAN. 16), I received my first update from RISKS in several years, under the same conditions, with my membership set to NOMAIL. Today, I received 80 messages from a LIST I had left (through NOMAIL) about four years ago and quickly sent an UNSUBSCRIBE message (which was acknowledged).

A student of mine has been doing research on a number of lists and a substantial fraction of the respondents tell about similar phenomena? Is the NOMAIL setting really a time bomb that may flood your mail directory unexpectedly? (I was fortunate in TELNETing from Berkeley today just as the avalanche had begun.) If you have an explanation of this process, I would appreciate hearing it.

Ron Ragsdale, Professor Emeritus, Ontario Institute for Studies in Education 252 Bloor Street West, Toronto, Ontario, Canada M5S 1V6 (416) 923-6641 X2252

Spontaneous recovery from "NOMAIL" setting?

"Peter M. Weiss" <PMW1@PSUVM.PSU.EDU> Sun, 23 Jan 1994 09:08:22 -0500 (EST)

List Management is more art than science ... I know, I'm a list-owner of multiple lists at multiple host locations. As good as the Revised LISTSERV software is, the list owners, users, and sysadmins can and do make mistakes (like the time I accidentally added another college president to a list that I maintained when I mistyped the userid).

One of the features of R-LISTSERV is for the owner to make changes to recipients' options, using various wild-card techniques ... without asking for confirmation, or for what the options were before they were set.

Also, a user can be subscribed under multiple userids, yet only receive a single distribution. Why? so that (s)he can post to a private distribution list from multiple sending addresses.

Peter M. Weiss, 31 Shields Bldg. -- Penn State Univ -- University Park, PA 16802-1202 +1 814 863 1843 pmw1@psuvm.psu.edu co-owner LDBASE-L, TQM-L, ...

Re: Verify your backups

rob horn <horn%temerity@leia.polaroid.com> 21 Jan 1994 17:42:49 -0500 (EST)

We have a practice that once per week we select one file at random and request that it be restored from backup from the previous week. It is amazing what you learn by doing this. The range of things that fail, problems that arise from odd causes, automatic systems that mysteriously stop working, is incredible. Even when all concerned know that this is the regular practice, things go wrong. So everyone who is willing to put in the time and effort to make backups should also perform at least this rudimentary QC check. Don't ever stop.

Rob Horn horn@temerity.polaroid.com

Bad backups (historical note)

Dick Hamlet <hamlet@cs.pdx.edu> Tue, 25 Jan 94 10:45:30 PST

The note from managers of wuarchive.wustl.edu about loss of archive files because backups were not usable reminds me of an experience with early DEC timesharing systems (c. 1968, 4-series PDP-10 operating system). (Incidently, why do I so often get the feeling that problems solved in the 1960s will reappear forever, and that each succeeding group of systems programmers has less time/talent/interest for attacking them?)

I was system programming director at Computer Center Corp. (C^3), a Seattle service bureau. We used 1/2" mag tape for backup of disk files. Only after we lost the entire disk did we discover that our sole mag tape unit (the cheapest we could buy, of course!) could not read all that it wrote, and that the dump/restore software ignored all tape errors! (This was the same system in which the FORTRAN library disk i-o routine did retry for read failure, but did it on the NEXT disk block instead of the one that had failed. It was remarkably successful—the were NO permanent failures ever logged!) Our fix for the backup program was to write checksums on tape. That way, we could check the tapes off line, and not slow the dump by doing a real file compare after the tape was written. How many dump systems today read back what has been written for backup (much less check it or do a file compare!) unless there is a restore request?

crypto policy report available online

"Lance J. Hoffman" <hoffman@seas.gwu.edu> Sat, 29 Jan 1994 09:04:55 -0500 (EST)

The following report is available by anonymous ftp from ftp.gwu.edu under directory /pub/hoffman. The document is stored under the name "cryptpol". It is a NIST-sponsored study.

The table of contents and abstract follows here.

CRYPTOGRAPHY: POLICY AND TECHNOLOGY TRENDS

Lance J. Hoffman, Faraz A. Ali, Steven L. Heckler, Ann Huybrechts

December 1, 1993

CONTENTS

EXECUTIVE SUMMARY

- 1. INTRODUCTION
- 2. TECHNOLOGY
- 3. MARKET ANALYSIS
- 4. EXPORT CONTROLS
- 5. PUBLIC POLICY ISSUES
 - 5.1 EXECUTIVE BRANCH
 - 5.2 CONGRESS
 - 5.3 TRENDS
- 6. POTENTIAL SCENARIOS

EXECUTIVE SUMMARY

During the past five years, encryption technology has become easily available to both individuals and businesses, affording them a level of security formerly available practically to only military, national security, and law enforcement agencies. As a result, a debate within the United States about the proper balance between national security and personal freedom has been initiated. Law enforcement and national security agencies would like to maintain tight control over civilian encryption technologies, while industry and individual and privacy rights advocates fight to expand their ability to distribute and use cryptographic products as they please.

This report analyzes trends in encryption technology, markets, export controls, and legislation. It identifies five trends which will have a strong influence on cryptography policy in the United States:

- * The continued expansion of the Internet and the progressive miniaturization of cryptographic hardware combined with the increasing availability and use of strong cryptographic software means that the strongest encryption technologies will continue to become more easily obtainable everywhere in the years ahead.
- * Additional growth in networked and wireless communication will fuel a strong demand for encryption hardware and software both domestically and abroad, causing the U. S. high-technology industry to be increasingly interested in selling encryption products overseas and in modifying current export restrictions.
- * Due to the responsibilities and bureaucratic dispositions of key Executive Branch agencies, products using strong encryption algorithms such as DES will continue to face at least some export restrictions, despite the widespread availability of strong encryption products overseas.
- * The American public is likely to become increasingly concerned about its privacy and about cryptographic policy as a result of the increased amount of personal information available online and the growing number of wireless and networked communications. The development and increasingly widespread use of the National Information Infrastructure will heighten these concerns.
- * Encryption policy is becoming an important public policy issue that will engage the attention of all branches of government. Congress will become increasingly visible in this debate due to its power of agency oversight and its role in passing laws accommodating the United States' rapid rate of technological change. Agencies will remain very important since they have the implementing and, often, the planning responsibilities. Since individuals and industry have more direct influence over Congress than over most other branches of government, Congress may place somewhat more emphasis on personal freedom than many other government actors.

Four potential scenarios are likely: mandatory escrowed encryption, voluntary

escrowed encryption, complete decontrol of encryption, or domestic decontrol with strict export regulations.

Professor Lance J. Hoffman, Dept of EECS, The George Washington University (202) 994-4955 Washington, D.C. 20052 hoffman@seas.gwu.edu Fax (202) 994-0227

✓ 1994 IEEE Symp on Research in Security and Privacy: PROGRAM

Catherine A. Meadows <meadows@itd.nrl.navy.mil> Fri, 28 Jan 94 18:15:03 EST

1994 IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY

May 16-18, 1994, Claremont Resort, Oakland, California

Sponsored by the IEEE Technical Committee on Security and Privacy In cooperation with the International Association of Cryptologic Research

Symposium Committee Cristi Garvey, General Chair Carl E. Landwehr, Vice Chair John Rushby, Program Co-Chair Catherine Meadows, Program Co-Chair

PRELIMINARY PROGRAM

MONDAY, MAY 16

9:15--9:30 Welcoming Remarks: Cristi Garvey and John Rushby

9:30--10:30 FORMAL MODELING OF CRYPTO PROTOCOLS

A Model for Secure Protocols and Their Compositions Nevin Heintze and J.D. Tygar (CMU) On Unifying Some Cryptographic Protocol Logics Paul Syverson (NRL) and Paul C. van Oorschot (BNR)

11:00--12:30 INFORMATION FLOW

Eliminating Formal Flows in Automated Information Flow Analysis Steven T. Eckmann (Unisys) Mode Security: An Infrastructure for Covert Channel Suppression Randy Browne (Independent Consultant) Simple Timing Channels Ira S. Moskowitz (NRL) and Allen R. Miller (GWU)

2:00--3:30 PANEL: Firewalls

4:00--5:00 COMPOSITION OF SECURE SYSTEMS

Asynchronous Composition and Required Security Conditions N. Boulahia-Cuppens and F. Cuppens (ONERA-CERT)

A General Theory of Composition for Trace Sets Closed under Selective Interleaving Functions, John McLean (NRL)

8:00: EVENING SESSIONS

TUESDAY, MAY 17

9:30--10:30 DATABASE I

Ensuring Data Security in Interrelated Tabular Data

Ram Kumar (U. North Carolina)

Collecting Garbage in Multilevel Secure Object Stores

Elisa Bertino (U. Milano), Luigi Mancini (U Genova), Sushil Jajodia (GMU)

11:00--12:30 CRYPTO ENGINEERING

Prudent Engineering Practice for Cryptographic Protocols

Martin Abadi (DEC-SRC) and Roger Needham (Cambridge)

Generating Formal Cryptographic Protocol Specifications

Ulf Carlsen (ENST de Bretagne)

A Low Cost, High Speed Encryption System and Method

Gregory Mayhew (Hughes Aircraft)

2:00--3:30 PANEL: What Security Needs To Learn From Other Fields

4:00--5:00 DATABASE II

Channel-Free Integrity Constraints in Multilevel Relational Databases

Xiaolei Qian (SRI-CSL)

Elimination of Inference Channels by Optimal Upgrading

Mark E. Stickel (SRI-AIC)

5:00: TC MEETING

8:00: EVENING SESSIONS

WEDNESDAY, MAY 18

9:30--10:30 DISTRIBUTED SYSTEMS

A Secure Group Membership Protocol, Michael K. Reiter (AT&T Bell Labs)

The Complexity and Composability of Secure Interoperation Li Gong and Xiaolei Qian (SRI-CSL)

11:00--12:30 ACCESS CONTROL

Self-Nonself Discrimination in a Computer

Stephanie Forrest, Allan Perelson, Lawrence Allen,

Rajesh Cherukuri (U New Mexico, Albuquerque)

Authentication and Revocation in SPM, Vijay Varadharajan (HP-Bristol)

On the Minimality of Testing for Rights in Transformation Models

Ravi S. Sandhu and Srinivas Ganta (GMU)

12:30: SYMPOSIUM ADJOURNS

1994 IEEE Symposium on Research in Security and Privacy

REGISTRATION FORM

Dates strictly enforced by postmark.	
Name:	
Affiliation:	
Postal Address:	
Phone:	
Fax:	
E-mail:	
Please enter the appropriate registration fee below:	
Advance Member (to 4/4/94)\$260	
IEEE Member # (REQUIRED)	
Late Member (4/5/94-4/22/94).\$310	
Advance Non-Member\$320	
Late Non-Member\$390	
Advance Student\$ 50	
Late Student\$ 50 Total amount due:	
Do you wish to present at a poster session or lead an evening discussion?	
[]Yes []No	
[]ICS []IVO	
Do you have any special requirements?	
Please indicate your method of payment by checking the appropriate box:	
<u> </u>	
Check in U.S. funds drawn on a U.S. bank (PLEASE ENCLOSE WITH THIS FORM)	
Condit and noth arisation.	
Credit card authorization:	
(Charges will appear on your statement as made by IEEE COMPUTER SOCIETY)	
Visa MasterCard American Express Diners Club	
_ _ _ _ _	
Credit Card Number:	
Card Holder Name:Expiration Date:	
Signature:	
	_
Mail registration to: Or fax this form (CREDIT CARD	
REGISTRATIONS ONLY) to:	
Code 5540A	
Naval Research Laboratory (202)404-7942	
12.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	
Washington, DC 20375-5337	

Evening Sessions



Hotel Reservations - The Claremont Resort

The Claremont Resort in Oakland, California is 20 minutes from San Francisco and just over an hour from Napa Valley. It is situated in the Oakland-Berkeley hills overlooking the San Francisco Bay on 22 acres of beautifully landscaped lawns and gardens. Facilities include the Claremont Pool and Tennis Club and The Spa at the Claremont.

Oakland Airport is 14 miles from the hotel, or attendees may choose to fly into San Francisco and rent a car. Bay Area Shuttle (415/873-7771) provides service from the San Francisco Airport or the Oakland Airport to the Claremont Resort. The charge is \$10 per person one way. Parking is available at the hotel at a cost of \$8 per day for guests and \$1.50 per hour up to a maximum of \$9 for non-guests.

Hotel reservations must be made under the group name IEEE Symposium on Research in Security and Privacy. The group rate is \$96 single, \$108 double occupancy, plus 11% tax. The cut-off date for reservations is Saturday, April 16, 1994. Reservations made after this date will be accepted on a space available basis. 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 non-refundable. Please be advised the check-in time is after 3:00 pm; check-out is 12 noon.

For reservations and information, contact: The Claremont Resort, Ashby and Domingo Avenues, Oakland, CA 94623-0363.

Phone: 510/843-3000; Fax: 510/843-6239.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 44

Weds 2 February 1994

Contents

Canada to monitor phone calls, fax, etc.?

Walter C. Daugherity

Risks of cliche collisions on the information superhighway Phil Agre

Irrational risk research

Phil Agre

Czech computer fraud

Mich Kabay

Clipper Petition

Dave Banisar

"Digital Woes" by Lauren Wiener

Rob Slade

Info on RISKS (comp.risks)

Canada to monitor phone calls, fax, etc.?

Walter C. Daugherity <daugher@chisholm.cs.tamu.edu> Wed, 2 Feb 94 09:04:52 -0600

>From EDUPAGE:

HIGH-TECH SNOOP GADGET. A super-secret branch of the Canadian Security Intelligence Service has awarded three contracts to a Montreal firm to make equipment that can quickly isolate key words and phrases from millions of airborne phone, fax, radio signals and other transmissions. The hardware has the "Orwellian potential to sweep through ... and keep records of all conversations," said one CSIS critic. (CTV National News, 01/31/94 11:00 pm).

Walter C. Daugherity, Texas A & M University, College Station, TX 77843-3112 Internet, NeXTmail: daugher@cs.tamu.edu uucp: uunet!cs.tamu.edu!daugher

Risks of cliche collisions on the information superhighway

Phil Agre <pagre@weber.ucsd.edu> Tue, 1 Feb 1994 12:06:51 -0800

The 1 Feb 1994 Wall Street Journal's front page center column is about the metaphors generated by the phrase "information superhighway", which (all are reported to agree) Al Gore coined by analogy to the US interstate highway system. What the article, like the vast majority of recent articles on the topic, is the whole point of the "highway" metaphor, which is the proposition that long-distance vehicle/information transfer may well be a natural monopoly, thus calling for the creation of some kind of public utility. This is a fairly spectacular example of the organized forgetting that goes on in the "agenda setting" process in US politics (and those, no doubt, of other countries, in their own ways). The risk here is that these semantical magic tricks may in the end deprive the public of the information infrastructure they deserve.

Evidence on this count is readily available, it so happens, in the 2/1/94 New York Times (business section, page C6), where we are told that investors are terrified that the Bell Atlantic - TCI merger might actually "lead to a destructively competitive "two-wire world", where phone and cable companies" would construct competing networks. Although the analysts are alarmed, Bell Atlantic has reassured its investors that it will be doing its best to avoid that scenario by focusing first on relatively high-profit (i.e., uncompetitive) markets.

Heads up.

Phil Agre, UCSD

[We are going to see all sorts of metaphors springing up on the InfoSuperhighway, such as speeding (illicit acts), speedtraps (network monitoring to detect misuse), parking lots (traffic congestion), StopAndShop (overload from 300 channels of home shopping), deprogramming services (for the compulsive shopper), and designated drivers (the device drivers you can trust). Maybe even BurmaShave signs scattering doggerel poetry along the way for the oldtimers. PGN]

irrational risk research

Phil Agre <pagre@weber.ucsd.edu> Tue, 1 Feb 1994 20:09:14 -0800

The 1 Feb 1994 New York Times (science section) includes an article by Daniel Goleman entitled "Hidden rules often distort ideas of risk". It's about a set of social psychological ideas about "perceptions" of risk that become newsworthy about once a year despite never seeming to change. These include the following:

- * Risks that are imposed loom larger than those that are voluntary.
- * Risks that seem unfairly shared are also seen as more hazardous.
- * Risks that people can take steps to control are more acceptable than those they feel are beyond their means to control.

- * Natural risks are less threatening than man-made ones.
- * Risks that are associated with catastrophes are especially frightening.
- * Risks from exotic technologies cause more dread than do those involving familiar ones.

The article reports a spectrum of views about the best explanation of these results and the best policies to deal with them. This spectrum might be categorized as follows:

Conservative: People are irrational, so forget 'em.

Moderate: People are irrational, but we can persuade them.

Liberal: People are irrational, but hey, everyone has faults, so let's humor them a little.

The common element, of course, is that is a view of ordinary people as irrational because their rankings of the risks from various technologies are considerably different from those of the experts.

What somehow never ceases to me is that all three approaches neglect a perfectly obvious explanation, which is that people distrust the institutions that seek to reassure them about unfamiliar technologies, having been repeatedly and egregiously lied to in the past by many of those same institutions (they were feeding plutonium to *whom*?), and they resent living in a world dominated by such institutions, so they refuse to acknowledge the claims of any technological project that has not been organized and evaluated in a democratic way. (The article does remark that people don't trust the numbers, but that's apparently because people irrationally fail to weigh the nuclear power plants that blow up against all the ones that don't.) Probably that's too simple, but it explains the data much more straightforwardly than the known alternatives.

The interesting sociological question is how this feat of conceptual constriction actually *works*. Does this explanation literally never occur to the people who do this research and write these articles? How can that be? Is it a conscious PR thing? That would be disappointing in a way (too straightforward), but it's certainly true enough with numerous other issues.

Clearly, as articles on the science pages so often conclude, further research is needed.

Phil Agre, UCSD

Czech computer fraud (More on RISKS-15.22)

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 30 Jan 94 14:53:20 EST

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

Czech-Computer Fraud

PRAGUE, Czech Republic (AP, 19 Jan 1994) -- A bank employee was sentenced to eight years in prison for stealing nearly \$1.2 million in the Czech Republic's first major computer fraud, a newspaper reported Wednesday. Martin Janku, an employee of the Czech Savings Bank in Sokolov, transferred money to his own account in the bank with the help of his own computer program between September 1991 and April 1992, the daily Mlada Fronta Dnes said.

The article continues with a few details:

- o Janku arrested when he tried to withdraw money from a branch where a teller recognized him as a programmer she'd met during training;
- o sentenced to 8 years in jail;
- o claims he was testing bank security;
- o returned about \$1 million of money he stole; rest, he says, was stolen from his car.

[Moral: never test someone's security systems without written authorization from the right people.]

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Clipper Petition

Dave Banisar <banisar@washofc.cpsr.org> Mon, 31 Jan 1994 15:59:20 EST

Electronic Petition to Oppose Clipper Please Distribute Widely

On January 24, many of the nation's leading experts in cryptography and computer security wrote President Clinton and asked him to withdraw the Clipper proposal.

The public response to the letter has been extremely favorable, including coverage in the New York Times and numerous computer and security trade magazines.

Many people have expressed interest in adding their names to the letter. In response to these requests, CPSR is organizing an Internet petition drive to oppose the Clipper proposal. We will deliver the signed petition to the White House, complete with the names of all the people who oppose Clipper.

To sign on to the letter, send a message to:

Clipper.petition@cpsr.org

with the message "I oppose Clipper" (no quotes)

You will receive a return message confirming your vote.

Please distribute this announcement so that others may also express their opposition to the Clipper proposal.

CPSR is a membership-based public interest organization. For membership information, please email cpsr@cpsr.org. For more information about Clipper, please consult the CPSR Internet Library - FTP/WAIS/Gopher CPSR.ORG /cpsr/privacy/crypto/clipper

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are writing to you regarding the "Clipper" escrowed encryption proposal now under consideration by the White House. We wish to express our concern about this plan and similar technical standards that may be proposed for the nation's communications infrastructure.

The current proposal was developed in secret by federal agencies primarily concerned about electronic surveillance, not privacy protection. Critical aspects of the plan remain classified and thus beyond public review.

The private sector and the public have expressed nearly unanimous opposition to Clipper. In the formal request for comments conducted by the Department of Commerce last year, less than a handful of respondents supported the plan. Several hundred opposed it.

If the plan goes forward, commercial firms that hope to develop new products will face extensive government obstacles. Cryptographers who wish to develop new privacy enhancing technologies will be discouraged. Citizens who anticipate that the progress of technology will enhance personal privacy will find their expectations unfulfilled.

Some have proposed that Clipper be adopted on a voluntary basis and suggest that other technical approaches will remain viable. The government, however, exerts enormous influence in the marketplace, and the likelihood that competing standards would survive is small. Few in the user community believe that the proposal would be truly voluntary.

The Clipper proposal should not be adopted. We believe that if this proposal and the associated standards go forward, even on a voluntary basis, privacy protection will be diminished, innovation will be slowed, government accountability will be lessened, and the openness necessary to ensure the successful development of the nation's communications infrastructure will be bthreatened.

We respectfully ask the White House to withdraw the Clipper proposal.



<"Rob Slade, Ed. DECrypt & ComNet, VARUG rep, 604-984-4067"> Mon, 31 Jan 1994 15:09:40 -0600 (MDT)

<ROBERTS@decus.ca>

Subject: "Digital Woes" by Lauren Wiener

Lauren Wiener, "Digital Woes", Addison-Wesley Publishing Co., 1993, 0-201-62609-8, U\$22.95/C\$29.95

When reviewing books on technical topics, one quickly learns to dread the work of those who do not actually practice in the field. (Yes, we are told that Wiener is a technical writer. They may very well be professionals, but the overwhelming majority are not technical professionals.) With this prejudice firmly in place, it came as a delightful surprise to find that "Digital Woes" is an accurate, well-researched, and thoroughly engaging treatment of the subject of software risks.

Chapter one is a list of specific examples of software failures, large and small. The stories are thoroughly documented and well told. The choice of examples is careful, and useful as well, covering a variety of problems. One could, of course, add to the list. In the virus field programs are extremely limited in function and rarely exceed 3000 bytes in length, yet almost every viral strain shows some programming pathology; most of the damage seems to be done by mistake. The user interfaces of antivirals are subject to hot debate, perhaps more importantly than in other systems because of the risks involved in misunderstanding. In regard to decision support, I recall the assumption, on the part of Excel, that everyone wants to use linear forecasting. Everyone involved in technical fields will be able to add other specific examples. For those uninvolved, Wiener's work is quite sufficient and convincing.

Chapter two is an explanation of why software contains bugs, and why software errors are so deadly. Techies will feel somewhat uncomfortable with the lack of jargon, but persevere. Initially, I thought she had missed the point of the difference between analogue and digital systems--until I realized I was in the middle of a complete and clear explanation that never had to use the word "analog". (Technopeasants will, of course, appreciate the lack of jargon. Rest assured that the same ease of reading and clarity of language holds throughout the book.)

Chapter three examines the various means used to try to ensure the reliability of software--usually with a depressing lack of success. As with all who have worked in the field, I can relate to the comments regarding the difficulty of testing. At one point I uncovered a bug in the third minor variant of the fourth major release of the fifth generation of a communications program. Apparently I was the first person on staff who had ever wanted to keep a running log between sessions--and the functions I used combined to completely lock up the computer.

Most RISKS-FORUM readers will by now be nodding and muttering, "So what else is new". However, Wiener here proves herself capable of some valuable and original contributions beyond the pronouncements of those working in the

field. Noting that she is familiar with programmers who have never, in twenty years of work, had their code incorporated into a delivered product, she raises the issue of what this type of work environment does to the psyche of the worker. My grandfather carved the wooden decorations in our church, and, fifty years after his death, I can still point that out. However, in a career of analysis, training and support, I can point to little beyond an amount of Internet bandwidth consumed. (Many would say "wasted".) To the ephemeral nature of the craft, though, one must add the legacy of constant failure. Martin Seligman's "Learned Helplessness" points out the danger quite clearly. A similar thought was voiced some years ago over the impact on developing youth of the then new video games, and the fact that you could advance through levels but never, ultimately, win. These children are grown now. You may know them as "Generation X".

Chapter four deals with means to prevent failure. Actually most of the material discusses recovery--assuming that the system will eventually fail, how to ensure that the failure causes the least damage.

Chapter five is entitled "Big Plans" and looks at various proposed new technologies and the risks inherent in them. In this discussion Wiener warns against those who are overly thrilled with the promises of the new technology. I agree, but I would caution that public debate is also dominated by those strident with fear. The arguments of both sides tend to entrench to defeat the opposition, while the public, itself, sits bemused in the middle without knowing whom to believe. It is a major strength of Wiener's work that the field is explored thoroughly and in an unbiased manner.

Many books which try to present an objective view of a controversial problem tend to trail off into meaningless weasel-words, but the final chapter here concerns "The Wise Use of Smart Stuff." Wiener lists a good set of criteria to use in evaluating a proposed system. The one item I would recommend be toned down is the axiom that personal care be excluded. I keep an old Berke Breathed "Bloom County" cartoon in my office wherein Opus, the Penguin, berates a computer for depriving him of his humanity until the bemused machine attempts to confirm that Opus is human. The perceived coldness of our institutions is often illusory. I once worked in a geriatric hospital and thought it a shame that our culture did not keep aging parents at home. Until, that is, I lived in a culture that did, and found that the "technology" of our hospitals provided more human contact to the old folks than did the "organic" home care. I also note that the belittled ELIZA is the only program to have passed the Turing test so far. A limited, unexpected, and hilarious pass, perhaps, but a pass nonetheless.

I note, as I am reviewing this book, a press release by a headhunting agency that half of all executives are computer illiterate. The survey method is extremely suspect, and I assume these figures are so kind as to be ridiculous. I would heartily recommend this work to technical and non-technical workers alike. Particularly, though, I recommend it to those executives who are the ones to make the ultimate decisions on major projects. Please re-read it after the next vendor demo you attend.

copyright Robert M. Slade, 1993 BKDGTLWO.RVW 931223

Postscriptum - my wife agrees with Peter Denning that I tend to editorialize in my reviews. This is likely true. "Digital Woes", however, deals with a topic which has prompted many editorials--and deals with it well.

Permission granted to distribute with unedited copies of the Digest

DECUS Canada Communications, Desktop, Education and Security group newsletters Editor and/or reviewer ROBERTS@decus.ca, RSlade@sfu.ca, Rob Slade at 1:153/733 DECUS Symposium '94, Vancouver, BC, Mar 1-3, 1994, contact: rulag@decus.ca



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 45

Tuesday 8 February 1994

Contents

- A Rise in Internet Break-ins Sets off a Security Alarm **NYT** excerpt
- CERT Advisory Ongoing Network Monitoring Attacks **CERT**
- "Misunderstanding" a CERT advisory Klaus Brunnstein
- Info on RISKS (comp.risks)

A RISE IN INTERNET BREAK-INS SETS OFF A SECURITY ALARM [Excerpt]

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 8 Feb 94 11:03:33 PST

By PETER H. LEWIS, c.1994 N.Y. Times News Service

NEW YORK Citing computer-security violations of unprecedented scope, security experts have issued a warning that unknown assailants have been breaking into scores of government, corporate and university computers connected to the global Internet communications network. Saying that it had been "flooded" with reports of computer break-ins in the last week, the federally supported Computer Emergency Response Team broadcast its warning late Thursday night over the Internet, a web of computer networks used by an estimated 15 million people in the United States and abroad.

Sophisticated software, secretly planted on various computers throughout the Internet, has allowed unknown intruders to steal passwords and electronic addresses from legitimate users, computer security experts said Friday.

[The full article summarizes a situation that by now should be familiar to RISKS readers. See the following CERT Advisory, and a comment from Klaus Brunnstein. See also articles the same day in the Washington Post and elsewhere. PGN]

CERT Advisory - Ongoing Network Monitoring Attacks

CERT Advisory <cert-advisory-request@cert.org> Thu, 3 Feb 94 21:14:40 EST

CA-94:01

CERT Advisory
February 3, 1994

Ongoing Network Monitoring Attacks

In the past week, CERT has observed a dramatic increase in reports of intruders monitoring network traffic. Systems of some service providers have been compromised, and all systems that offer remote access through rlogin, telnet, and FTP are at risk. Intruders have already captured access information for tens of thousands of systems across the Internet.

The current attacks involve a network monitoring tool that uses the promiscuous mode of a specific network interface, /dev/nit, to capture host and user authentication information on all newly opened FTP, telnet, and rlogin sessions.

In the short-term, CERT recommends that all users on sites that offer remote access change passwords on any network-accessed account. In addition, all sites having systems that support the /dev/nit interface should disable this feature if it is not used and attempt to prevent unauthorized access if the feature is necessary. A procedure for accomplishing this is described in Section III.B.2 below. Systems known to support the interface are SunOS 4.x (Sun3 and Sun4 architectures) and Solbourne systems; there may be others. Sun Solaris systems do not support the /dev/nit interface. If you have a system other than Sun or Solbourne, contact your vendor to find if this interface is supported.

While the current attack is specific to /dev/nit, the short-term workaround does not constitute a solution. The best long-term solution currently available for this attack is to reduce or eliminate the transmission of reusable passwords in clear-text over the network.

I. Description

Root-compromised systems that support a promiscuous network interface are being used by intruders to collect host and user authentication information visible on the network.

The intruders first penetrate a system and gain root access through an unpatched vulnerability (solutions and workarounds for these vulnerabilities have been described in previous CERT advisories, which are available anonymous FTP from info.cert.org).

The intruders then run a network monitoring tool that captures up to the first 128 keystrokes of all newly opened FTP, telnet, and rlogin sessions visible within the compromised system's domain. These keystrokes usually contain host, account, and password

information for user accounts on other systems; the intruders log these for later retrieval. The intruders typically install Trojan horse programs to support subsequent access to the compromised system and to hide their network monitoring process.

II. Impact

All connected network sites that use the network to access remote systems are at risk from this attack.

All user account and password information derived from FTP, telnet, and rlogin sessions and passing through the same network as the compromised host could be disclosed.

III. Approach

There are three steps in CERT's recommended approach to the problem:

- Detect if the network monitoring tool is running on any of your hosts that support a promiscuous network interface.
- Protect against this attack either by disabling the network interface for those systems that do not use this feature or by attempting to prevent unauthorized use of the feature on systems where this interface is necessary.
- Scope the extent of the attack and recover in the event that the network monitoring tool is discovered.

A. Detection

The network monitoring tool can be run under a variety of process names and log to a variety of filenames. Thus, the best method for detecting the tool is to look for 1) Trojan horse programs commonly used in conjunction with this attack, 2) any suspect processes running on the system, and 3) the unauthorized use of /dev/nit.

1) Trojan horse programs:

The intruders have been found to replace one or more of the following programs with a Trojan horse version in conjunction with this attack:

/usr/etc/in.telnetd and /bin/login - Used to provide back-door access for the intruders to retrieve information /bin/ps - Used to disguise the network monitoring process

Because the intruders install Trojan horse variations of standard UNIX commands, CERT recommends not using other

commands such as the standard UNIX sum(1) or cmp(1) commands to locate the Trojan horse programs on the system until these programs can be restored from distribution media, run from read-only media (such as a mounted CD-ROM), or verified using cryptographic checksum information.

In addition to the possibility of having the checksum programs replaced by the intruders, the Trojan horse programs mentioned above may have been engineered to produce the same standard checksum and timestamp as the legitimate version. Because of this, the standard UNIX sum(1) command and the timestamps associated with the programs are not sufficient to determine whether the programs have been replaced.

CERT recommends that you use both the /usr/5bin/sum and /bin/sum commands to compare against the distribution media and assure that the programs have not been replaced. The use of cmp(1), MD5, Tripwire (only if the baseline checksums were created on a distribution system), and other cryptographic checksum tools are also sufficient to detect these Trojan horse programs, provided these programs were not available for modification by the intruder. If the distribution is available on CD-ROM or other read-only device, it may be possible to compare against these volumes or run programs off these media.

2) Suspect processes:

Although the name of the network monitoring tool can vary from attack to attack, it is possible to detect a suspect process running as root using ps(1) or other process-listing commands. Until the ps(1) command has been verified against distribution media, it should not be relied upon--a Trojan horse version is being used by the intruders to hide the monitoring process. Some process names that have been observed are sendmail, es, and in.netd. The arguments to the process also provide an indication of where the log file is located. If the "-F" flag is set on the process, the filename following indicates the location of the log file used for the collection of authentication information for later retrieval by the intruders.

3) Unauthorized use of /dev/nit:

If the network monitoring tool is currently running on your system, it is possible to detect this by checking for unauthorized use of the /dev/nit interface. CERT has created a minimal tool for this purpose. The source code for this tool is available via anonymous FTP on info.cert.org in the /pub/tools/cpm directory or on ftp.uu.net in the /pub/security/cpm directory as cpm.1.0.tar.Z. The checksum information is:

Filename	Standard UNIX S	Sum System V Sum
cpm.1.0.tar.Z:	11097 6	24453 12

MD5 Checksum

MD5 (cpm.1.0.tar.Z) = e29d43f3a86e647f7ff2aa453329a155

This archive contains a readme file, also included as Appendix C of this advisory, containing instructions on installing and using this detection tool.

B. Prevention

There are two actions that are effective in preventing this attack. A long-term solution requires eliminating transmission of clear-text passwords on the network. For this specific attack, however, a short-term workaround exists. Both of these are described below.

1) Long-term prevention:

CERT recognizes that the only effective long-term solution to prevent these attacks is by not transmitting reusable clear-text passwords on the network. CERT has collected some information on relevant technologies. This information is included as Appendix B in this advisory. Note: These solutions will not protect against transient or remote access transmission of clear-text passwords through the network.

Until everyone connected to your network is using the above technologies, your policy should allow only authorized users and programs access to promiscuous network interfaces. The tool described in Section III.A.3 above may be helpful in verifying this restricted access.

2) Short-term workaround:

Regardless of whether the network monitoring software is detected on your system, CERT recommends that ALL SITES take action to prevent unauthorized network monitoring on their systems. You can do this either by removing the interface, if it is not used on the system or by attempting to prevent the misuse of this interface.

For systems other than Sun and Solbourne, contact your vendor to find out if promiscuous mode network access is supported and, if so, what is the recommended method to disable or monitor this feature.

For SunOS 4.x and Solbourne systems, the promiscuous interface to the network can be eliminated by removing the /dev/nit capability from the kernel. The procedure for doing so is outlined below (see your system manuals for more details). Once the procedure is complete, you may remove the

device file /dev/nit since it is no longer functional.

Procedure for removing /dev/nit from the kernel:

- 1. Become root on the system.
- 2. Apply "method 1" as outlined in the System and Network Administration manual, in the section, "Sun System Administration Procedures," Chapter 9, "Reconfiguring the System Kernel." Excerpts from the method are reproduced below:

```
# cd /usr/kvm/sys/sun[3,3x,4,4c]/conf
# cp CONFIG_FILE SYS_NAME
```

[Note that at this step, you should replace the CONFIG_FILE with your system specific configuration file if one exists.]

```
# chmod +w SYS_NAME
# vi SYS_NAME
```

```
# # The following are for streams NIT support. NIT is used by # etherfind, traffic, rarpd, and ndbootd. As a rule of thumb, # NIT is almost always needed on a server and almost never # needed on a diskless client. # pseudo-device snit # streams NIT
```

pseudo-device pf # packet filter
pseudo-device nbuf # NIT buffering module

[Comment out the preceding three lines; save and exit the editor before proceeding.]

```
# config SYS_NAME
# cd ../SYS_NAME
# make
# mv /vmunix /vmunix.old
# cp vmunix /vmunix
# /etc/halt
> b
```

[This step will reboot the system with the new kernel.]

[NOTE that even after the new kernel is installed, you need to take care to ensure that the previous vmunix.old , or other kernel, is not used to reboot the system.]

C. Scope and recovery

If you detect the network monitoring software at your site, CERT recommends following three steps to successfully determine the scope of the problem and to recover from this attack.

1. Restore the system that was subjected to the network monitoring software.

The systems on which the network monitoring and/or Trojan horse programs are found have been compromised at the root level; your system configuration may have been altered. See Appendix A of this advisory for help with recovery.

2. Consider changing router, server, and privileged account passwords due to the wide-spread nature of these attacks.

Since this threat involves monitoring remote connections, take care to change these passwords using some mechanism other than remote telnet, rlogin, or FTP access.

3. Urge users to change passwords on local and remote accounts.

Users who access accounts using telnet, rlogin, or FTP either to or from systems within the compromised domain should change their passwords after the intruder's network monitor has been disabled.

4. Notify remote sites connected from or through the local domain of the network compromise.

Encourage the remote sites to check their systems for unauthorized activity. Be aware that if your site routes network traffic between external domains, both of these domains may have been compromised by the network monitoring software.

The CERT Coordination Center thanks the members of the FIRST community as well as the many technical experts around the Internet who participated in creating this advisory. Special thanks to Eugene Spafford of Purdue University for his contributions.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

Internet E-mail: cert@cert.org

Telephone: 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.

CERT Coordination Center

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 info.cert.org.

Appendix A:

RECOVERING FROM A UNIX ROOT COMPROMISE

- A. Immediate recovery technique
 - 1) Disconnect from the network or operate the system in single- user mode during the recovery. This will keep users and intruders from accessing the system.
 - 2) Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as cmp(1) located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX sum(1) program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

-- or --

Reload your system from the vendor's media.

3) Search the system for new or modified setuid root files.

find / -user root -perm -4000 -print

If you are using NFS or AFS file systems, use ncheck to search the local file systems.

ncheck -s /dev/sd0a

- 4) Change the password on all accounts.
- 5) Don't trust your backups for reloading any file used by root. You do not want to re-introduce files altered by an intruder.
- B. Improving the security of your system
 - 1) CERT Security Checklist

Using the checklist will help you identify security weaknesses or modifications to your systems. The CERT Security Checklist is based on information gained from computer security incidents reported to CERT. It is available via anonymous FTP from info.cert.org in the file pub/tech_tips/security_info.

2) Security Tools

Use security tools such as COPS and Tripwire to check for security configuration weaknesses and for modifications made by intruders. We suggest storing these security tools, their configuration files, and databases offline or encrypted. TCP daemon wrapper programs provide additional logging and access control. These tools are available via anonymous FTP from info.cert.org in the pub/tools directory.

3) CERT Advisories

Review past CERT advisories (both vendor-specific and generic) and install all appropriate patches or workarounds as described in the advisories. CERT advisories and other security-related information are available via anonymous FTP from info.cert.org in the pub/cert_advisories directory.

To join the CERT Advisory mailing list, send a request to:

cert-advisory-request@cert.org

Please include contact information, including a telephone number.

CERT Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890

Copyright (c) Carnegie Mellon University 1994																													
				_	_				_	_	_	_	_	_	_	_	_	_					_	_	_	_	_	_	_

Appendix B:

ONE-TIME PASSWORDS

Given today's networked environments, CERT recommends that sites concerned about the security and integrity of their systems and networks consider moving away from standard, reusable passwords. CERT has seen many incidents involving Trojan network programs (e.g., telnet and rlogin) and network packet sniffing programs. These programs capture clear-text hostname, account name, password triplets. Intruders can use the captured information for subsequent access to those hosts and accounts. This is possible because 1) the password is used over and over (hence the term "reusable"), and 2) the password

passes across the network in clear text.

Several authentication techniques have been developed that address this problem. Among these techniques are challenge-response technologies that provide passwords that are only used once (commonly called one-time passwords). This document provides a list of sources for products that provide this capability. The decision to use a product is the responsibility of each organization, and each organization should perform its own evaluation and selection.

I. Public Domain packages

S/KEY(TM)

The S/KEY package is publicly available (no fee) via anonymous FTP from:

thumper.bellcore.com /pub/nmh directory

There are three subdirectories:

skey UNIX code and documents on S/KEY.
Includes the change needed to login,
and stand-alone commands (such as "key"),
that computes the one-time password for
the user, given the secret password and
the S/KEY command.

dos DOS or DOS/WINDOWS S/KEY programs. Includes DOS version of "key" and "termkey" which is a TSR program.

mac One-time password calculation utility for the Mac.

II. Commercial Products

Secure Net Key (SNK) (Do-it-yourself project)

Digital Pathways, Inc. 201 Ravendale Dr. Mountain View, Ca. 94043-5216 USA

Phone: 415-964-0707 Fax: (415) 961-7487

Products:

handheld authentication calculators (SNK004) serial line auth interrupters (guardian)

Note: Secure Net Key (SNK) is des-based, and therefore restricted from US export.

Secure ID (complete turnkey systems)

Security Dynamics
One Alewife Center
Cambridge, MA 02140-2312
USA

Phone: 617-547-7820 Fax: (617) 354-8836

Products:

SecurID changing number authentication card ACE server software

SecureID is time-synchronized using a 'proprietary' number generation algorithm

WatchWord and WatchWord II

Racal-Guardata 480 Spring Park Place Herndon, VA 22070 703-471-0892 1-800-521-6261 ext 217

Products:

Watchword authentication calculator Encrypting modems

Alpha-numeric keypad, digital signature capability

SafeWord

Enigma Logic, Inc. 2151 Salvio #301 Concord, CA 94520 510-827-5707 Fax: (510)827-2593

Products:

DES Silver card authentication calculator SafeWord Multisync card authentication calculator

Available for UNIX, VMS, MVS, MS-DOS, Tandum, Stratus, as well as other OS versions. Supports one-time passwords and super smartcards from several vendors.

Appendix C:

cpm 1.0 README FILE

cpm - check for network interfaces in promiscuous mode.

Copyright (c) Carnegie Mellon University 1994 Thursday Feb 3 1994

CERT Coordination Center

Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890

This program is free software; you can distribute it and/or modify it as long as you retain the Carnegie Mellon copyright statement.

It can be obtained via anonymous FTP from info.cert.org:pub/tools/cpm.tar.Z.

This program is distributed WITHOUT ANY WARRANTY; without the IMPLIED WARRANTY of merchantability or fitness for a particular purpose.

This package contains:

README

MANIFEST

cpm.1

cpm.c

To create cpm under SunOS, type:

% cc -Bstatic -o cpm cpm.c

On machines that support dynamic loading, such as Sun's, CERT recommends that programs be statically linked so that this feature is disabled.

CERT recommends that after you install cpm in your favorite directory, you take measures to ensure the integrity of the program by noting the size and checksums of the source code and resulting binary.

The following is an example of the output of cpm and its exit status.

Running cpm on a machine where both the le0 and le2 interfaces are in promiscuous mode, under csh(1):

% cpm

le0

le2

% echo \$status

2

%

Running cpm on a machine where no interfaces are in promiscuous mode, under csh(1):

% cpm

% echo \$status

0

%

"Misunderstanding" a CERT advisory

Klaus Brunnstein

Strunnstein@rz.informatik.uni-hamburg.d400.de>
Mon, 7 Feb 1994 16:37:14 +0100

Waves went high in some German media on Friday, Feb.5 1994, when news from Philadelphia (via CMU-SEI's press release) and Washington's Post was mediated by some European news agencies. Germany's 2nd TV channel (ZDF) informed the surprised public that *hackers had succeeded to invade a secure network which had been installed in times of Cold War to protect US Armed Forces even in the case of a Nuclear War*. As several 10,000 passwords had been hacked, now more than 20 million users have to change their password. Regional and private TV and radio stations followed on Saturday, though only few newspapers took this up on Monday.

Nothing of this (mis)information was in the CERT advisory distributed on Febrary 3, where users of some UNIX systems (esp. SunOS with /dev/nit) were informed that it might be wise to take precautionary action against a potential sniffer attack. Now, 3 days later, responsible journalists inform us that there were *2 agency reports*, one delivered by German press agency (dpa) which was rather serious and non-speculative, and another one from Agency France Press (AFP) which ZDF based it's report upon (as it was the more "interesting one:-). Here is this in-famous text (translation by messenger):

"Washington, February 5 (AFP) - Computer pirates have cracked the largest computer network in the world. Totally 20 million users on 'Internet' should receive new passwords, told the emergency committee installed by US ministry of defence. Internet is used by universities, government agencies, enterprises and private persons. The network was established in times of the Cold War to serve US Armed Forces also in case of Atomic War as 'invulnerable' information network. The hackers, so far unidentified, succeeded according to the emergency committee to read data from ten thousands of systems on 'Internet'. They succeeded by using a program named 'Trojan Horse' which allows legal access to Internet central computer but then does not go any further."

Apart from the many wrong or misunderstood facts in this news, the reaction of some experts was interesting. German Information Agency (GISA) said: "Old stuff, no reason panic!" Another expert said: "CERT is in actual fight for money from US administration, they needed some public attention!" General comments were: "Blind actionism of US' CERT!"

Somehow, the media uproar reminds of the Michelangelo case where cautious warnings of experts (infection at most small percentage of PCs) were publicly raised *up to 50 mio infected PC systems* by badly informed journalists. No expert can ever exclude that her/his warnings are always correctly understood, but in this case, the serious question is: With so many unknown parameters (how many different sniffer trojans existed? How many nodes were affected? For what purposes were the sniffers used? etc): why issued CERT/CC a press release (which it very rarely did so far), in addition to its advisory?

Unfortunately, this unjustified media hysteria will fall back, as in previous cases, on those who work hard for improving security and safety of systems and networks:-) This is why the background must be carefully analysed.

Klaus Brunnstein (Feb.7,1994)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 46

Tuesday 8 February 1994

Contents

Medical privacy violation

Mich Kabay

Revised Documents on FTP server without version number

David W. Crawford

Campaign Against Clipper

Dave Banisar

Re: Clipper Petition

David Gursky

Don't trust the phone company

Tom Bodine

Modern discussion of computer risks in old book

Lauren Wiener

RISKs of network surveys

Craig DeForest

National Cryptology Museum

Larry Hunter

10th ACSAC Call for Papers

Vince Reed

Info on RISKS (comp.risks)

Medical privacy violation

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 06 Feb 94 21:32:00 EST

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

Health Care-Privacy, By MARCY GORDON, Associated Press Writer WASHINGTON (AP, 27 Jan 1994) -- In a clear, quiet voice welling with emotion, Rep. Nydia Velazquez told a Senate hearing Thursday how hospital records related to her suicide attempt were leaked to New York newspapers during her election campaign. Velazquez, a New York Democrat, testified before a Senate Judiciary subcommittee hearing on how President Clinton's

proposed health plan would protect the privacy of medical records."

The author continues with details of the hearing. Key points:

- o Sen. Patrick Leahy, D-Vt., chair of the subcommittee on technology and the law, warned that the Clinton proposals would result in a nationwide computerized database holding confidential data.
- Nan Hunter, deputy general counsel of the Department of Health and Human Services, said, "[T]he administration is committed to privacy as a first principle and the need to protect the confidentiality of these records."
- Misuse of medical card numbers would result in criminal and civil penalties.
- Velazquez discovered that her medical records had been sent by anonymous fax to several newspapers, resulting in front-page headlines about her attempted suicide.
- o According to Velazquez, there are no federal regulations controlling the use of medical records that escape from doctors' offices.
- o Leahy mentioned that Arthur Ashe' medical records also became public.
- Janlori Goldman, director of the American Civil Liberties Union's privacy and technology project, warned of the importance of safeguarding "the privacy and security of personal health information."
- Carolyn Roberts, chairwoman-elect of the American Hospital Association, commented on the wide disparities in state legislation protecting health information against unauthorized disclosure. She argued for a new federal privacy law to supersede state laws.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Revised Documents on FTP server without version number

David W. Crawford <crawford@fido.econlab.arizona.edu> Mon, 07 Feb 1994 16:29:29 -0700 (MST)

>From croberts@crl.com Mon Feb 7 09:47:09 1994

Newsgroups: alt.internet.services

Subject: Altered White House documents

Date: 5 Feb 1994 09:38:23 -0800

I assume everyone knows about the ftp site whitehouse.gov. I just discovered that the Clinton rebuttal to Elizabeth McCaughey's critique of his health care plan has been altered on whitehouse.gov - with no mention in the current version that it has been changed.

According to Associated Press writer Tom Raum, the original White House

rebuttal to McCaughey's New Republic magazine article used the word "lie" four times. The copy of the White House rebuttal I just downloaded (Feb 5, morning, pacific time) does not contain the word lie nor does it contain any indication that it is a "revised" version.

White House spokesman Dee Dee Myers defended the rebuttal on Thursday although she conceded that "perhaps the language was a little strong." Clinton, asked by reporters earlier this week about calling McCaughey's comments lies, responded, "Well, I hate to use that word, but the New Republic article was way off base and the New Republic didn't make total disclosure about the source of the article." So Clinton admitted to the use of "lie" but it has since been removed from the version available for anonymous ftp at whitehouse.gov. Makes you wonder just how self- serving and accurate the rest of the information there might be...

UWSA'ers note: the whitehouse.gov directory /pub/political-science/speeches/perot contains the text of Perot's book "United We Stand," and various Perot speeches. But no, I have not double-checked them for unauthorized "revisions."

From: Samer Farha <Samer@clark.net> Newsgroups: alt.internet.services writes:

In almost every speech (be it a minute or an hour) every member of Congress starts off by saying words to the effect of "I would like to reserve the right to extend and revise my remarks", which is followed by the chair saying that "without objection, it is agreed to.."

This little phrase gives any speaker the right to add pages of a speech, when they only have two minutes left in official debate. That way, when someone says, but you got up there and said only one thing, the Congressman can say that is not true: look at the daily record, it has the whole speech. Often, they may say something in a less than articulate way and then revise the way the said it for the record.

One time two Senators got into a very heated name calling session, it was reported in the press and seen on C-SPAN, but it was removed from the official record after they both calmed down and "revised" their remarks.

People will always change their minds or regret saying something, they often try to tell you that what they meant was not what they said. If they are rich or powerful enough, they will hire press agents to "spin" the story the right way. This changing of printed documents is nothing but an extension of that. The media is there to make sure that big glaring mess ups don't fall through the cracks.

David Crawford crawford@Arizona.EDU, U of Arizona

Campaign Against Clipper

Dave Banisar <banisar@washofc.cpsr.org>

Mon, 7 Feb 1994 22:28:08 EST

CPSR ANNOUNCES CAMPAIGN TO OPPOSE CLIPPER PROPOSAL

Embargoed until 2 pm, Monday, February 7, 1994

contact: rotenberg@washofc.cpsr.org (202 544 9240)

Washington, DC -- Following the White House decision on Friday to endorse a secret surveillance standard for the information highway, Computer Professionals for Social Responsibility (CPSR) today announced a national campaign to oppose the government plan.

The Clipper proposal, developed in secret by the National Security Agency, is a technical standard that will make it easier for government agents to wiretap the emerging data highway.

Industry groups, professional associations and civil liberties organizations have expressed almost unanimous opposition to the plan since it was first proposed in April 1993.

According to Marc Rotenberg, CPSR Washington director, the Administration made a major blunder with Clipper. "The public does not like Clipper and will not accept it. This proposal is fatally flawed."

CPSR cited several problems with the Clipper plan:

- o The technical standard is subject to misuse and compromise. It would provide government agents with copies of the keys that protect electronic communications. "It is a nightmare for computer security," said CPSR Policy Analyst Dave Banisar.
- o The underlying technology was developed in secret by the NSA, an intelligence agency responsible for electronic eavesdropping, not privacy protection. Congressional investigations in the 1970s disclosed widespread NSA abuses, including the illegal interception of millions of cables sent by American citizens.
- o Computer security experts question the integrity of the technology. Clipper was developed in secret and its specifications are classified. CPSR has sued the government seeking public disclosure of the Clipper scheme.
- o NSA overstepped its legal authority in developing the standard. A 1987 law explicitly limits the intelligence agency's power to set standards for the nation's communications network.
- o There is no evidence to support law enforcement's claims that new technologies are hampering criminal investigations. CPSR recently forced the release of FBI documents that show no such problems.
- o The Administration ignored the overwhelming opposition of the general public. When the Commerce Department solicited public comments on the proposal last fall, hundreds of people opposed the plan while only a few expressed support.

CPSR today announced four goals for its campaign to oppose the Clipper initiative:

o First, to educate the public about the implications of the Clipper proposal.

o Second, to encourage people to express their views on the Clipper proposal, particularly through the computer network.

Toward that goal, CPSR has already begun an electronic petition on the Internet computer network urging the President to withdraw the Clipper proposal. In less than one week, the CPSR campaign has drawn thousands of electronic mail messages expressing concern about Clipper. To sign on, email clipper.petition@cpsr.org with the message "I oppose clipper" in the body of the text.

o Third, to pursue litigation to force the public disclosure of documents concerning the Clipper proposal and to test the legality of the Department of Commerce's decision to endorse the plan.

o Fourth, to examine alternative approaches to Clipper.

Mr. Rotenberg said "We want the public to understand the full implications of this plan. Today it is only a few experts and industry groups that understand the proposal. But the consequences of Clipper will touch everyone. It will affect medical payments, cable television service, and everything in between.

CPSR is a membership-based public interest organization. For more information about CPSR, send email to cpsr@cpsr.org or call 415 322 3778. For more information about Clipper, check the CPSR Internet library CPSR.ORG. FTP/WAIS/Gopher and listserv access are available.

★ Re: Clipper Petition

David Gursky <dgursky@nextsrv1.andi.org> Fri, 4 Feb 94 18:31 EST

- > Electronic Petition to Oppose Clipper
- > Please Distribute Widely

<Text of petition solicitation removed to save bandwidth>

>To sign on to the letter, send a message to:

> Clipper.petition@cpsr.org

>with the message "I oppose Clipper" (no quotes)

>You will receive a return message confirming your vote.

I apologize for sounding sarcastic or cynical, but I was quite chagrined when I saw this proposal appear in RISKS. Not because I am opposed to what

CPSR proposes in the message, but rather:

- 1 Because the risks associated with electronic voting have been well discussed in this forum and
- 2 Because the Computer Professionals for Social Responsibility, an organization that ought to know better, (certainly with a name like theirs), does not appear to have included any mechanism in their their petition drive to mitigate these risks.

Now I'll certainly grant that the CPSR's petition has no rule of law behind it, as would a petition to put a local ordinance on an election ballot, but the irony of CPSR's request is noteworthy.

[Given the inherent risks of spoofing E-mail, there is clearly a risk of someone sending a bogus petition signature. In the absence of nontrivial authentication, there is always the option of human verification... PGN]

Don't trust the phone company

Tom Bodine <tbodine@utig.ig.utexas.edu> 8 Feb 1994 13:53:35 GMT

I am the victim of false accusations.

My wife and I were at home some time last week. I was busy cooking dinner. My wife was busy chasing our two year old, when we received a phone call which my wife accepted. The fellow on the other end of the line was extremely irate. His wife has been receiving obscene phone calls for some time now. He had purchased the service provided by the phone company which allows you to call back the last person to dial you. After his wife had discontinued the obscene call she'd just received, he had used this feature to righteously confront her abuser. Instead he had dialed us.

This was somewhat perplexing until a few minutes later, my wife's best friend called. Imediately after saying hello, My wife began relating this strange occurence to her friend. Her friend then told my wife that it was her husband who had made this call utilizing this phone service.

This has put a heavy strain upon my wife's relationship with her friend, because her friend's husband has assumed that I am the author of these obscene calls. Whereas I barely have time for all the things which fill my life. I have no time or interest in making such calls.

It is my belief that my wife had tried to call her best friend during the obscene phone call. This attempt overwrote the perpetrator's number, so that when the call back service was used, our phone rang instead.

If there are any knowledgeable netter's out there that could give me any more info, I'd appreciate it.

Regards Tom Bodine

modern discussion of computer risks in old book

Lauren Wiener <lauren@reed.edu> Wed, 02 Feb 94 21:47:22 -0800

My uncle was poking around in a used bookstore and found a book entitled "The Naked Computer" (by Jack Rochester & John Gantz, Wm Morrow & Co., NY) which was published in 1983 and intended for a lay audience. It's got some stories I have never heard, such as this one on p. 71:

"David Walonick, a computer programmer and consultant in Minneapolis, found that his new IBM personal computer divided 0.1 by 10 and came up with 0.001 instead of 0.01. IBM told him beginning programmers "have problems like that." It wasn't corrected until Walonick told the _New York Times_."

There follows a somewhat muddy and unsatisfying explanation of the problem, followed by the insightful comment:

"The more serious problem is that most computer users have difficulty discerning when there is an inaccurate sum; computers are generally regarded as correct."

The book also includes an interview by Adam Osborne, in which he says the following on the subject of computer risks:

"Authors: In your book, _Running Wild_, you say there are places we shouldn't use computers.

"Osborne: Yes. In balloting, for instance, I just feel that the slightest chance of fraud isn't worth it. If we are going to spend a little bit more money for counting or if we have to wait longer, fine. We all know that rigging is possible -- it's very easy to do. It's not just the outsiders I'm worried about, it's the people running it.

"Electronic funds transfer is the next place where I have a lot of problems because the potential for fraud is so great. I've heard of banks that are doing funds transfer on public-access networks. In 1980 I issued a public challenge to any bank that would guarantee in writing not to prosecute me that I would steal \$10 million from them via wire fraud. We weren't actually going to rip off the bank; in fact, we were going to call the bank president and ask him to come and get his money. We'd have a \$10 million cashier's check waiting for him. Of course, no bank took me up on the offer.

As for the stock exchange, my God! There has never been an opportunity like that. Who is going to count the shares? Who really knows who owes who what? I think it's madness."

Wonder what he thinks now?

RISKs of network surveys

Craig "Powderkeg" DeForest <zowie@daedalus.stanford.edu> 3 Feb 94 00:17:07

I subscribe to the Presidential-speech service from CLINTON.ai.mit.edu. I've been getting electronic copies of all Clinton's speeches since before his election (when I also got Bush's speeches).

A couple of days ago, I got a letter from "M.I.T. Pollster's Assistant", asking me to fill out a survey about my usage of the service. I, of course, complied.

There was some confusion about one of the questions -- I gave the server an invalid answer, and it wrote me back asking me for a correction to that particular question only.

I sent back the form -- but apparently the server misunderstood, because I got back *another* polite auto-letter telling me I'd filed an incomplete survey, and would I please fill out the remaining seven questions?

Confused, I decided to make a wash of the whole thing. I have done nothing for one week.

I just received a letter from the server, asking me to finish filling out my survey! Not surprising, except that the 40-odd line message was preceded by 250 lines of "Apparently-To: <hapless-fool@some.other.machine>". Apparently, all of us hapless fools are in the same boat, but now ALL OF THEM know that I am one of "those" undesirable sorts of people who start filling out surveys and then don't finish them. In fact, I (and they) can surmise that everyone on the list receives the clinton service. In a matter of seconds, I had several of their true names via finger -- as, I imagine, they did mine. Mild annoyance -- here, privacy is more a matter of courtesy than necessity -- but it's easy to imagine a situation that called for more anonymity (say a sexual preferences survey).

To sum up: (A) public mail-servers have to be not only clever and polite, but also extremely robust; and (B) it's very easy to compromise list privacy by mistake.

Fortunately, I'm in good company. Two lines below me is BIFF@MIT.EDU, another truant survey-taker! KOOL, EH?!!1!

National Cryptology Museum

Larry Hunter <hunter@work.nlm.nih.gov> Thu, 3 Feb 94 14:08:06 -0500

Following up on Jeremy Epstein's note in <u>RISKS 15.41</u>, I went to visit the National Cryptology Museum, and can recommend it. It's open 9am-3pm weekdays and by appointment. It's basically one large room, with several interesting

displays; my favorite was 7 volumes from the NSA rare book collection, including the oldest published work on cryptology, Johannes Trithemius' "Polygraphiae," first published in 1517. They also had a Pace-10 analog computer, and IBM Harvest and a Cray XMP-24 on display. There were nice historical displays on Yarley & the Black Chamber, US Civil War crypto and a US Revolutionary War era crypto device (the M-94) that may have been designed by Thomas Jefferson. The largest display was dedicated to Enigma and the device for cracking it, Bombe. There is a working Enigma that visitors can use! There are a few displays that are more current: pictures of the NSA buildings and director and a description of NSA's Special Processing Lab (SPL) which does special purpose chip fabrication. There was the expected KGB stuff, and a quote from George Washington about the importance of "keeping the whole matter secret."

The curator, Jack Ingrams, was friendly and eager to answer (some) questions. He said that since the Washington Post article, traffic had been about 25-30 people a day, and that they will be on TV this week, which he expects to further increase the number of visitors. He was curious about the RISKS posting and internet, so if anybody who sees this talks to him while visiting, mention the net. He also said that they will be opening the unclassified portion of their crypto library to scholars sometime in the summer. The handout on the museum also says that the FOIA reading room shares space with the library.

Obligatory RISK-y note: Ingrams mentioned that the museum opened to NSA personnel in October, and to the general public around Christmas time. A quick glance through the guest sign-in book shows that the fourth visitor to the museum, on October 29, was one Duane Whitlock, who listed his employer as C&P Telephone, our local baby bell. hmmm.

10th ACSAC Call for Papers

<vreed@smiley.mitre.org>
Tue, 8 Feb 1994 08:56:30 -0600

CALL FOR PAPERS AND PARTICIPATION
Tenth Annual Computer Security
Applications Conference
December 5-9, 1994
Orlando, Florida

With the advent of the Information Age, information systems are routinely processing private, proprietary, sensitive, classified, and critical information. Computers have created a universal addiction to information in the military, government, and private sectors. The result is a proliferation of computers, computer networks, databases, and applications empowered to make decisions ranging from the mundane to life threatening or life preserving.

Some of the computer security challenges that the community is faced with include the following:

* Develop methodologies and tools for designing systems capable of

protecting the sensitivity and integrity of information, and assuring that expected services are available when needed.

- * Design safety-critical systems such that their software and hardware are not hazardous.
- * Develop methodologies and tools capable of assuring that computer systems accorded trust are worthy of that trust.
- * Build systems of systems out of components that have been deemed trustworthy.
- * Build applications on evaluated trusted systems without compromising the inherent trust.
- * Include computer security in enterprise modeling and reengineering.
- * Extend computer security technologies to specifically address the needs of the civil and private sectors.
- * Develop international standards for computer security technology.

This conference will attempt to address these challenges. It will explore a broad range of technology applications with security and safety concerns. Technical papers, panels, vendor presentations, and tutorials that address the application of computer security and safety technologies in the civil, defense, and commercial environments are solicited. Selected papers will be those that present examples of in-place or attempted solutions to these problems in real applications; lessons learned; and original research, analyses, and approaches for defining the computer security issues and problems. Of particular interest are papers that present descriptions of secure systems in use or under development, general strategy, methodologies for analyzing the scope and nature of integrated computer security issues, and potential solutions. Papers written by students will be judged for a Best Student Paper Award. A prize of \$500, plus expenses to attend the conference, will be awarded for the selected best student paper (contact the Student Paper Award Chairperson for details, but submit your paper to the Technical Program Chairperson).

Panels of interest include those that present alternative/ controversial viewpoints or those that encourage lively discussion of relevant issues. Panels that are simply a collection of unrefereed papers will not be selected.

Vendor presentations of interest should emphasize innovative product implementations, especially implementations involving the integration of multiple products. Vendor presentations that simply describe product features will not be selected.

INSTRUCTIONS TO AUTHORS

Send five copies of your paper or panel proposal to Dr. Gary Smith, Technical Program Chair, at the address given below. Since we provide blind refereeing, we ask that you put names and affiliations of authors on a separate cover page only. Substantially identical papers that have been previously published or are under consideration for publication elsewhere should not be submitted. Panel proposals should be a minimum of one page that describes the panel theme and appropriateness of the panel for this conference, as well as identifies panel participants and their respective viewpoints. For panel/forum preparation instructions, please contact Jody Heaney at (703) 883-5837 or via e-mail at heaney@smiley.mitre.org. Send five copies of your vendor presentation proposal to Steve Rome at the address given below. Vendor presentation proposals should include an abstract and outline that describe the product and example applications. Send one copy of your tutorial proposal to Daniel Faigin at the address given below. It should consist of one- to two-paragraph abstract of the tutorial, an initial outline of the material to be presented, and an indication of the desired tutorial length (full day or half day). Electronic submission of tutorial proposals is preferred.

Completed papers as well as proposals for panels, vendor presentations, and tutorials must be received by May 31, 1994. Authors will be required to certify prior to June 30, 1994, that all necessary clearances for public release have been obtained; that the author or qualified representative will be represented at the conference to deliver the paper, and that the paper has not been accepted elsewhere. Authors will be notified of acceptance by August 5, 1994. Camera-ready copies are due not later than September 26, 1994. Material should be sent to:

Dr. Gary Smith Daniel Faigin

Technical Program Chair

ARCA Systems, Inc.

8229 Boone Blvd., Suite 610

Vienna, VA 22182

Tutorial Program Chair

The Aerospace Corporation

P.O. Box 92957, MS M1/055

Los Angeles, CA 90009-2957

(703) 734-5611 (310) 336-8228 smith@arca.va.com faigin@aero.org

Steve Rome Ravi Sandhu

Vendor Track Chair Student Paper Award
CISS, Code TGD George Mason University
5113 Leesburg Pike, Suite 400 ISSE Department
Falls Church, VA 22041 Fairfax, VA 22030-4444

(703) 756-7926 (703) 993-1659

romes@cc.ims.disa.mil sandhu@gmuvax2.gmu.edu

Areas of Interest Include

Computer Security Tools
Software Safety Analysis and Design
Trusted System Architectures and Technology
Encryption Applications (e.g., Digital Signature)
Application of Formal Assurance Methods
Risk/Hazard Assessments
Security Policy and Management Issues
Security in Enterprise Modeling or Reengineering
Trusted DBMSs, Operating Systems, and Networks

Open Systems and Composted Systems Electronic Document Interchange Certification, Evaluation, and Accreditation

Additional Information

For more information or to receive future mailings, please contact the following at:

Ann Marmor-Squires Vince Reed
Conference Chair Publicity Cochair

TRW Systems Division The MITRE Corporation

1 Federal Systems Park Drive 1500 Perimeter Pkwy., Suite 310

Fairfax, VA 22033 Huntsville, AL 35806 (703) 803-5503 (205) 830-2606 marmor@charm.isi.edu vreed@mitre.org



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 47

Weds 9 February 1994

Contents

"Sounding the Alarm: Noisy medical alert systems"

B Fitler

(Semi-)electronic locks

Pete Kaiser

Safety in Telescript, Part Deux

Luis Valente

Risks of email exacerbating typos

M. Hedlund

Patents Hearing as it relates to Software

Paul Robinson

Network surveys et al.

Steve Holzworth

Re: Don't Trust The Phone Company

Lars Poulsen

Re: "Misunderstanding" a CERT advisory

D.R. Newman

Re: Clipper Petition

Pete Kaiser

John Mainwaring

Re: Altered White House Documents

Firth

Larry Nathanson

EFF Wants You (to add your voice to the crypto fight!)

Stanton McCandlish

Info on RISKS (comp.risks)

"Sounding the Alarm: Noisy medical alert systems"

<bfitler@ccmail.com>

Tue, 08 Feb 94 19:05:55 pst

Article titled "Sounding the Alarm: Noisy medical alert systems are getting out of hand" by Jon Van, Chicago Tribune, appeared in San Jose Mercury News Science & Medicine Section 8 Feb 1994.

The article pointed out the alarm systems from medical equipment are "driving doctors and nurses to distraction" who agree that "alarm noise pollution is a significant problem that threatens patient health" presumably because "doctors order that all alarms be disconnected except those deemed absolutely necessary for patient safety."

Points raised in the article:

- * Efforts to create international standards for alarms have been underway since 1983 and are still unfinished.
- * "...it is common for one event, such as a drop in a patient's blood pressure or speeding of his heart's rate, to set off a cascade of alarms from several sources..."
- * "... conditions change during surgery, and medical equipment isn't able to distinguish context..."
- * "... typically the attorney or chief executive [of the medical equipment manufacturer] thinks that the louder the alarm, the less likely their company is to be sued if someone doesn't respond..."
- * Manufacturers see legal problems in trying to tie together warning systems from a variety of medical systems.

The article did not point out the technical difficulties involved in prioritizing alarm conditions.

(Semi-)electronic locks

Technology Strategy & Architecture <kaiser@heron.enet.dec.com> Wed, 9 Feb 94 08:18:15 MET

The "New Scientist" for 6 February 1993 contains this article:

Chips hold key to door security

An electronic key with a chip in its tip is to be marketed by the locksmiths, Chubb Security of Sunbury-on-Thames. The key, called Eloctro, has a tiny silicon chip which stores a unique number ranging from 10 to 70 000 billion.

The key fits a special battery-powered lock which stores all the authorised numbers in a memory chip. When a key is inserted, the lock generates an electromagnetic field, which is picked up by an antenna on the chip. The antenna switches on the chip, allowing the lock to read the key's unique number. If the number matches one in the lock's memory the key can turn.

The numbers in the lock's memory can be stored individually, by inserting a controllor's key followed by the numbered key; or, a

computer can load a list of authorised numbers.

Although individually numbered swipe cards have been available for years storing the number on a chip is more secure because it is almost impossible to read or reprogramme the number without breaking the key. It is not available for homes yet.

Several rather evident risks there.

___Pete kaiser@heron.vbo.dec.com +33 92.95.62.97 FAX +33 92.95.50.50

Safety in Telescript, Part Deux

"Luis Valente" <luis_valente@genmagic.genmagic.com> 31 Jan 1994 10:54:14 -0800

Following my posting to RISKS on January 17 entitled "Safety in Telescript" a number of readers have strongly questioned some of the statements I made in that posting. Two of those statements, in which I used casual or imprecise language, were particularly criticized:

1- "Telescript is interpreted and, thus, is safer than compiled languages." As pointed out by many readers, an interpreted language is not intrinsically safer than a compiled language. It is the Telescript language definition that provides that protection. Within the abstraction created by Telescript, programs lack operations for directly manipulating the physical resources of the "real" computer(s) on which they execute.

That doesn't mean that Telescript programs cannot interact with applications (e.g., databases) outside the Telescript abstraction.

However, that interaction can only take place via Telescript objects that act as proxies for the "external" applications. Each such proxy object defines the features of the corresponding external application that are to be made available to Telescript agents and places. It may also define and enforce a security policy for controlling access to those features (e.g., based on an agent's credentials and permit). Furthermore, the administrative authority for a given Telescript engine is capable of controlling (by means of mechanisms built into the language) who can and cannot create these proxy objects.

2- "Authority names are cryptographically generated and cannot be forged." Obviously, that statement is not true in an absolute sense since the "unforgeability" of the authority name is directly related to the cryptographic mechanism used to generate it. We currently use RSA-based public key cryptography for generating authority names. Entitlement to use a particular authority name can be linked to the secret key used to generate it.

Aside from the criticism leveled against my poor choice of words in the aforementioned statements, several readers complained about the lack of more detailed information on the security technology used by Telescript, namely, what cryptographic algorithms are used, key sizes, key

distribution and management issues, exportability issues, etc.

Let me start by saying that my posting was not meant as a treatise on Telescript Technology but merely a brief description of some of the features of Telescript that can be used effectively against misprogrammed or ill-intentioned telescripts.

General Magic has already published a white paper entitled "Telescript Technology: The Foundation of the Electronic Marketplace." This paper provides a high-level description of Telescript and is intended for the layman, not the techno-savvy reader. It can be requested directly from General Magic by calling (415) 965-0400. In the coming months we will publish additional information on many different aspects of Telescript Technology (including security).

Let me further say that the point of my original posting was not that Telescripted networks are intrinsically secure (i.e., the "it won't happen here" syndrome). It was simply to let RISKS readers know that we have put a lot of thought into the security aspects of Telescript. In fact, when General Magic started developing Telescript, security was at the top of our list of concerns. As a result, we have built into the fabric of the language a number of features that, we believe, will enable application developers to write safe Telescript programs and network operators to run highly secure Telescripted networks.

Heretofore, the discussions on RISKS have only covered a few of the many security issues faced by a dynamic, interpreted, communication-centric language like Telescript. As more detailed information on Telescript becomes widely available, I am certain it will generate heated debates on this and other forums. I look forward to them!

-Luis Valente, General Magic, Inc.

Risks of email exacerbating typos

M. Hedlund <hedlund@netcom.com> Tue, 8 Feb 1994 20:03:17 GMT

>From the New York Times, Tuesday, February 8, p. C5:

E-mail apparently made a bad situation worse for Bon Marche, a department store in Washington, Oregon, Idaho, Montana, and Wyoming. The store misprinted a sale price for a Sony five-disk carousel CD player as \$99, when it was intended to be \$179 (on sale from \$199). The NYT reports that nearly 5,000 people took advantage of the misprint, some placing paid orders once available stock had been sold.

One salesman called attention to an unusual risk of email:

The surge came in part because some employees at the Microsoft Corporation, based in nearby Redmond, had mentioned the deal in electronic-mail messages, he said.

Although the store could have run a correction ad or posted a disclaimer, they did not; the price, according to the senior VP for marketing John Buller, "was not totally irrational for this product." I suppose the risk shouldn't keep us up nights.

M. Hedlund

✓ Patents Hearing as it relates to Software

Paul Robinson <PAUL@TDR.COM> Tue, 8 Feb 1994 22:23:46 -0500 (EST)

Those of you on the West Coast be advised that there will be a hearing on the issue of Patents as they relate to the issues of software development. The hearing is scheduled for February 10, in Room J of the San Jose Convention Center, San Jose California, starting at 9:00 or so.

There will be a subsequent hearing on the East Coast a couple of days later, near the Patent Office in Crystal City, Virginia.

A copy of the notice as published in the Federal Register (about 45K) was posted to several lists on the Internet almost a month ago. It is possible to go to the hearing(s) to see them, but it is too late to sign up to speak, I believe. However, comments on the Federal Register notice may be E-Mailed to Jeff Kushan kushan@uspto.gov>.

Paul Robinson - Paul@TDR.COM

Network surveys et al.

Steve Holzworth <sch@unx.sas.com> Wed, 9 Feb 1994 11:29:30 -0500 (EST)

Craig DeForest (zowie@daedalus.stanford.edu) describes how an automated survey daemon managed to show him a list of other subscribers to a political-speech service. I had a similar, but more serious incident occur on my account with a commercial Internet access provider.

The access provider (approximately 1000 users), in the interests of security, routinely runs one of the many password cracking programs against their /etc/passwd file. One day, I received Email stating that my password was weak (it was). The interesting thing about the Email is that it included a list of all recipients of the same message; the To: field was a concatenated string of all users with weak passwords...

I sent Email to the operator, advising that this might not be the best strategy for dealing with the problem :-). He assured me that this was a one-time slip, due to his having used a Email command that improperly included the full distribution list... Sigh.

The site DOES use a shadow password file, so it's not as bad as it could be.

Steve Holzworth

sch@unx.sas.com "Do not attribute to poor spelling "Do stattribute to poor spelling "That which is actually poor typing..."

SAS/Macintosh Development Team - me

Cary, N.C.

★ Re: Don't Trust The Phone Company (Bodine, RISKS-15.46)

Lars Poulsen <lars@eskimo.CPH.CMC.COM> Wed, 9 Feb 94 14:03:35 +0100

Tom Bodine reports the unsettling experience of being accused of making an obscene phone call, after the husband of the recipient of the call (his wife's best friend) used the "call return" feature at the end of the obscene call, and then reached his number. He speculates that his number was captured by the friend's telephone switch as the result of a failed call from his wife while the friend's line was busy with the obscene call.

While such a feature interaction is possible (is the number supposed to be captured on a busy? I know it is on a no-answer failure), there is another way for this to occur: The perpetrator may have applied the call forwarding feature on his own phone prior to making the call, and left it there for a bit afterwards. In this situation, the number that was captured would not be the Bodines', but that of the perpetrator. The effect would be the same, however, except that if the call is a billable long distance call, the number would show up on the next phone bill, and in the case of forwarding it would be the perpetrator's number (since the last leg of the call is billed to the forwarding phone).

I believe that there is no such interaction problem in the case of the "calling number identification" feature, since the number is delivered in real time and only when the call rings through. Thus, the call that would come in DURING the problem call, would only be recorded if the recipient had the "call waiting" feature, and in that case would not get busy, but ringback, and the CNID (if subscribed) would be delivered between the rings (call waiting tones)).

I am forwarding this note to the TELECOM DIGEST where someone from AT&T or Bellcore will probably be able to look up whether the mechanism surmised by Tom Bodine is also possible. I hope that this technical information will go some way towards repairing relations between the families.

★ Re: "Misunderstanding" a CERT advisory

"D.R.NEWMAN" <FIG0008@v2.qub.ac.uk> Wed, 9 Feb 94 18:55 GMT

Expect journalistic exaggeration. 2 people died in a cyclone on the island of Mauritius in the 1970s. In the Kenyan papers this was 20 - in

the British papers 200. Now if CERT sued for libel and got damages, that might get the journalists to check their facts!

Dr. David R. Newman, Queen's University, Information Management Dept., BELFAST BT7 1NN, Northern Ireland. <d.r.newman@qub.ac.uk>

★ Re: Clipper Petition

Technology Strategy & Architecture <kaiser@heron.enet.dec.com> Wed, 9 Feb 94 08:28:38 MET

Someone of my acquaintance (who doesn't care to be identified here) sent in a response to CPSR's Clipper petition and received a full and explanatory confirmation from CPSR at the address from which it was sent. So if CPSR is also culling out signatures from bogus addresses, those two measures together are a good beginning.

___Pete kaiser@heron.vbo.dec.com +33 92.95.62.97 FAX +33 92.95.50.50

Re: Clipper Petition

"john (j.g.) mainwaring" <crm312a@bnr.ca> Wed, 9 Feb 1994 11:11:00 +0000

In Risks issue 46, David Gursky mentions the possibility that some of the responses to the CPSR petition will be of the "Vote early, vote often" variety, and goes on to cite previous discussion of the risks of dial up voting.

Petitions are not votes. CPSR does not claim to be collecting votes on Clipper and tallying the ayes, nays and throat clearings. Petitions are an unsupervised form of expression. The older paper variety could be padded pretty easily too. Other risks associated with petitions (electronic or not) include the possibility of bias in the question to manipulate response: "Even though the President claims to have stopped beating his wife, it is the opinion of responsible rabble rousers in this great country that..." Anybody who's been in politics even as long as our present youthful president knows that petitions can be manipulated, and adds salt accordingly.

The theatrical value of collecting a petition about the electronic superhighway in the rest stops of the present byways is obvious. The strong risk that the petition will include invalid responses needs to be weighed against the risk of having an unnecessarily expensive and possibly untrustworthy security system in future. Or does anyone believe that Clipper would make collecting petitions safe from democracy?

★ Re: Altered White House Documents (Roberts/Crawford, RISKS-15.46)

<firth@SEI.CMU.EDU>

Wed, 9 Feb 94 10:39:22 -0500

<u>RISKS-15.46</u> reports on how an electronic document available from whitehouse.gov was surreptitiously changed without any visible audit trail.

The relevant quote came to mind immediately:

"He who controls the past controls the future."

I believe the answer is an independent party that will daily download all documents from this site and systematically scan for similar attempts to revise history.

★ Re: Altered White House Documents (Roberts/Crawford, RISKS-15.46)

Larry Nathanson <lan@panix.com> 8 Feb 1994 17:26:04 -0500

Perhaps a site on the net with a little bit of spare disk space would like to mirror this site??? I know I'd find the 'diff's more informative than the speeches themselves.

EFF Wants You (to add your voice to the crypto fight!)

Stanton McCandlish <mech@eff.org> 7 Feb 1994 17:34:17 -0600

The Electronic Frontier Foundation needs your help to ensure privacy rights!

* DISTRIBUTE WIDELY *

Monday, February 7th, 1994

From: Jerry Berman, Executive Director of EFF, jberman@eff.org

Dear Friends on the Electronic Frontier,

I'm writing a personal letter to you because the time has now come for action. On Friday, February 4, 1994, the Administration announced that it plans to proceed on every front to make the Clipper Chip encryption scheme a national standard, and to discourage the development and sale of alternative powerful encryption technologies. If the government succeeds in this effort, the resulting blow to individual freedom and privacy could be immeasurable.

As you know, over the last three years, we at EFF have worked to ensure freedom and privacy on the Net. Now I'm writing to let you know about something *you* can do to support freedom and privacy. *Please take a moment to send e-mail to U.S. Rep. Maria Cantwell (cantwell@eff.org) to show your support of H.R. 3627, her bill to liberalize export controls on encryption software.* I believe this bill is critical to empowering

ordinary citizens to use strong encryption, as well as to ensuring that the U.S. software industry remains competitive in world markets.

Here are some facts about the bill:

Rep. Cantwell introduced H.R. 3627 in the House of Representatives on November 22, 1993. H.R. 3627 would amend the Export Control Act to move authority over the export of nonmilitary software with encryption capabilities from the Secretary of State (where the intelligence community traditionally has stalled such exports) to the Secretary of Commerce. The bill would also invalidate the current license requirements for nonmilitary software containing encryption capabilities, unless there is substantial evidence that the software will be diverted, modified or re-exported to a military or terroristic end-use.

If this bill is passed, it will greatly increase the availability of secure software for ordinary citizens. Currently, software developers do not include strong encryption capabilities in their products, because the State Department refuses to license for export any encryption technology that the NSA can't decipher. Developing two products, one with less secure exportable encryption, would lead to costly duplication of effort, so even software developed for sale in this country doesn't offer maximum security. There is also a legitimate concern that software companies will simply set up branches outside of this country to avoid the export restrictions, costing American jobs.

The lack of widespread commercial encryption products means that it will be very easy for the federal government to set its own standard--the Clipper Chip standard. As you may know, the government's Clipper Chip initiative is designed to set an encryption standard where the government holds the keys to our private conversations. Together with the Digital Telephony bill, which is aimed at making our telephone and computer networks "wiretap-friendly," the Clipper Chip marks a dramatic new effort on the part of the government to prevent us from being able to engage in truly private conversations.

We've been fighting Clipper Chip and Digital Telephony in the policy arena and will continue to do so. But there's another way to fight those initiatives, and that's to make sure that powerful alternative encryption technologies are in the hands of any citizen who wants to use them. The government hopes that, by pushing the Clipper Chip in every way short of explicitly banning alternative technologies, it can limit your choices for secure communications.

Here's what you can do:

I urge you to write to Rep. Cantwell today at cantwell@eff.org. In the Subject header of your message, type "I support HR 3627." In the body of your message, express your reasons for supporting the bill. EFF will deliver printouts of all letters to Rep. Cantwell. With a strong showing of support from the Net community, Rep. Cantwell can tell her colleagues on Capitol Hill that encryption is not only an industry concern, but also a grassroots issue. *Again: remember to put "I support HR 3627" in your Subject header.*

This is the first step in a larger campaign to counter the efforts of those who would restrict our ability to speak freely and with privacy. Please stay tuned--we'll continue to inform you of things you can do to promote the removal of restrictions on encryption.

In the meantime, you can make your voice heard--it's as easy as e-mail. Write to cantwell@eff.org today.

Sincerely,

Jerry Berman, Executive Director, EFF jberman@eff.org

P.S. If you want additional information about the Cantwell bill, send e-mail to cantwell-info@eff.org. To join EFF, write membership@eff.org. For introductory info about EFF, send any message to info@eff.org.

The text of the Cantwell bill can be found on the Internet with the any of the following URLs (Universal Resource Locaters):

ftp://ftp.eff.org/pub/Policy/Legislation/cantwell.bill http://www.eff.org/ftp/EFF/Policy/Legislation/cantwell.bill gopher://gopher.eff.org/00/EFF/legislation/cantwell.bill

It will be available on AOL (keyword EFF) and CIS (go EFFSIG) soon.

From: Stanton McCandlish <mech@eff.org>

Subject: Administration adopts coldwar mentality, pushes for Clipper

EFF Press Release Feb 4 '94 * DISTRIBUTE WIDELY *

At two briefings, Feb. 4, 1994, the Clinton Administration and various agencies gave statements before a Congressional committee, and later representatives of civil liberties organizations, industry spokespersons and privacy advocates. The Electronic Frontier Foundation's position, based on what we have seen and heard from the Administration today, is that the White House is set on a course that pursues Cold War national security and law enforcement interests to the detriment of individual privacy and civil liberties.

The news is grim. The Administration is:

- * not backing down on Clipper
- * not backing down on key escrow
- * not backing down on selection of escrow agents
- * already adamant on escrowed key access procedures
- * not willing to eliminate ITAR restrictions
- * hiding behind exaggerated threats of "drug dealers" and "terrorists"

The material released to the industry and advocacy version of the briefing have been placed online at ftp.eff.org (long before their online availability from government access sites, one might add). See below for specific details.

No information regarding the Congressional committee version of the briefing has been announced. EFF Director Jerry Berman, who attended the private sector meeting, reported the following:

"The White House and other officials briefed industry on its Clipper chip and encryption review. While the review is not yet complete, they have reached several policy conclusions. First, Clipper will be proposed as a new Federal Information Processing Standard (FIPS) next Wednesday. [Feb. 9] It will be "voluntary" for government agencies and the private sector to use. They are actively asking other vendors to jump in to make the market a Clipper market. Export licensing processes will be speeded up but export restrictions will not be lifted in the interests of national security. The reason was stated bluntly at the briefing: to frustrate competition with clipper by other powerful encryption schemes by making them difficult to market, and to "prevent" strong encryption from leaving the country thus supposedly making the job of law enforcement and intelligence more difficult. Again in the interest of national security. Of course, Clipper will be exportable but they would not comment on how other governments will view this. Treasury and NIST will be the escrow agents and Justice asserted that there was no necessity for legislation to implement the escrow procedures.

"I asked if there would be a report to explain the rationale for choosing these results - we have no explanation of the Administration's thinking, or any brief in support of the results. They replied that there would be no report because they have been unable to write one, due to the complexity of the issue.

"One Administration spokesperson said this was the Bosnia of Telecommunications. I asked, if this was so, how, in the absence of some policy explanation, could we know if our policy here will be as successful as our policy in Bosnia?"

The announcements, authorization procedures for release of escrowed keys, and q-and-a documents from the private sector briefing are online at EFF.

They are:

"Statement of the [White House] Press Secretary" [White House] file://ftp.eff.org/pub/EFF/Policy/Crypto/wh_press_secy.statement

"Statement of the Vice President" [very short - WH] file://ftp.eff.org/pub/EFF/Policy/Crypto/gore_crypto.statement

"Attorney General Makes Key Escrow Encryption Announcements" [Dept. of Just.] file://ftp.eff.org/pub/EFF/Policy/Crypto/reno_key_escrow.statement

"Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III/State Statutes/FISA"
[3 docs. in one file - DoJ]
file://ftp.eff.org/pub/EFF/Policy/Crypto/doj_escrow_intercept.rules

"Working Group on Data Security" [WH] file://ftp.eff.org/pub/EFF/Policy/Crypto/interagency_workgroup.announce

"Statement of Dr. Martha Harris Dep. Asst. Secy. of State for Polit.-Mil. Affairs: Encryption - Export Control Reform" [Dept. of State] file://ftp.eff.org/pub/EFF/Policy/Crypto/harris_export.statement

"Questions and Answers about the Clinton Administration's Encryption Policy" [WH] file://ftp.eff.org/pub/EFF/Policy/Crypto/wh_crypto.q-a

These files are available via anonymous ftp, or via WWW at: http://www.eff.org/ in the "EFF ftp site" menu off the front page.

Gopher access:

gopher://gopher.eff.org/

Look in "EFF Files"/"Papers and Testimony"/"Crypto"

All 7 of these documents will be posted widely on the net immediately following this notice.

Contacts:

Digital Privacy: Jerry Berman, Exec. Director <jberman@eff.org>
Daniel J. Weitzner, Sr. Staff Counsel <djw@eff.org>
Archives: Stanton McCandlish, Online Activist <mech@eff.org>
General EFF Information: info@eff.org

From: Stanton McCandlish <mech@eff.org>

Subject: EFF Cantwell campaign update - a torrent of responses

EFF's "Letter to Cantwell" campaign, to collect and send letters to Rep. Cantwell in support of her bill to ease export restrictions on cryptography, collected more that *five hundred* responses the first day along, and at 5pmEST Tue. (2/8/94), was gaining more at a rate approaching 100 per *hour*.

To add your voice to this clear signal to Rep. Cantwell that her legislation (bill HR 3627) is on the right track, send a message with a subject line of "Subject: I support HR 3627" to cantwell@eff.org

Stanton McCandlish * mech@eff.org * Electronic Frontier Found. OnlineActivist

INFO@EFF.ORG FOR INFO: OPEN PLATFORM, ONLINE RIGHTS, VIRTUAL CULTURE, CRYPTO



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 48

Weds 9 February 1994

Contents

- Notes on key escrow meeting with NSA **Matt Blaze**
- Re: Campaign and Petition Against Clipper **Dorothy Denning**
- Information on RISKS comp.risks
- Info on RISKS (comp.risks)

Notes on key escrow meeting with NSA

Matt Blaze <mab@research.att.com> Tue, 08 Feb 94 16:03:55 -0500

(originally submitted last week, but lost somewhere in our news system)

A group from NSA and FBI met the other day with a group of us at Bell Labs to discuss the key escrow proposal. They were surprisingly forthcoming and open to discussion and debate, and were willing to at least listen to hard questions. They didn't object when asked if we could summarize what we learned to the net. Incidentally, the people at the meeting seemed to base a large part of their understanding of public opinion on Usenet postings. Postings to RISKS, sci.crypt and talk.politics.crypto seem to actually have an influence on our government.

Since the many of the points brought up at the meeting have been discussed in RISKS, it seems appropriate to post a summary here.

A number of things came out at the meeting that we didn't previously know or that clarified previously released information. What follows is a rough summary; needless to say, nothing here should be taken as gospel, or representing the official positions of anybody. Also, nothing here should be taken as an endorsement of key escrow, clipper, or anything else by the authors; we're just reporting. These notes are based on the collective memory of Steve Bellovin, Matt Blaze, Jack Lacy, and Mike Reiter; there may be errors

or misunderstandings. Please forgive the rough style. Note also the use of "~ ~" for 'approximate quotes' (a marvelous Whit Diffie-ism).

NSA's stated goals and motives for all this:

- * DES is at the end of its useful life
- * Sensitive, unclassified government data needs protection
- * This should be made available to US Citizens
- * US business data abroad especially needs protection
- * The new technology should not preclude law enforcement access

They indicated that the thinking was not that criminals would use key escrowed crypto, but that they should not field a system that criminals could easily use against them. The existence of key escrow would deter them from using crypto in the first place. The FBI representative said that they expect to catch "~only the stupid criminals~" through the escrow system.

Another stated reason for key escrow is that they do not think that even government-spec crypto devices can be kept physically secure. They do expect enough to be diverted to the black market that they feel they need a response. NSA's emphasis was on the foreign black market...

There seems to be a desire to manipulate the market, by having the fixed cost of key escrow cryptography amortized over the government market. Any private sector devices would have to sell a much larger number of units to compete on price. (This was somewhere between an implication and an explicit statement on their part.)

When asked about cryptography in software, "~...if you want US government cryptography, you must do it with hardware~".

The NSA people were asked whether they would consider evaluating ciphers submitted by the private sector as opposed to simply proposing a new cipher as a "black box" as they did with Skipjack. They said they can't do this because, among other things, of the extraordinary effort required to properly test a new cipher. They said that it often takes from 8-12 years to design, evaluate and certify a new algorithm, and that Skipjack began development "~about 10 years ago.~" I asked if we should infer anything from that about the value of the (limited time and resource) civilian Skipjack review. They accepted the question with good humor, but they did say that the civilian review was at least presented with and able to evaluate some of the results of NSA's previous internal reviews.

Clipper chips should be available (to product vendors) in June. You can't just buy loose chips - they have to be installed in approved products. Your application interface has to be approved by NIST for you to get your hands on the chips.

An interesting point came up about the reverse-engineering resistance of the chips: they are designed to resist non-destructive reverse engineering. It was not clear (from the information presented at the meeting) whether the chips are equally resistant to destructive reverse-engineering. That is, the chips are designed to resist non-destructive reverse engineering to obtain the unit keys. They do not believe that it is possible to obtain the unit key of a particular chip without destroying the chip. They did not present any

assertions about resistance to destructive reverse engineering, such that several chips can be taken apart and destroyed in the process, to learn the Skipjack algorithm. They said the algorithm was patented, but they may have been joking. ("~And if that doesn't scare you enough, we'll turn the patent over to PKP.~")

The resistance to reverse engineering is not considered absolute by NSA. They do feel that "~it would require the resources of a national laboratory, and anyone with that much money can design their own cryptosystem that's just as strong.~"

They repeated several times that there are "~no plans to regulate the use of alternate encryption within the US by US citizens.~" They also indicated they "~weren't naive~" and didn't think that they could if they wanted to.

There were 919 authorized wiretaps, and 10,000 pen register monitors, in 1992. They do not have any figures yet on how often cryptography was used to frustrate wiretaps.

They do not yet have a production version of the "decoder" box used by law enforcement. Initially, the family key will be split (by the same XOR method) and handled by two different people in the authorized agencies. There is presently only one family key. The specifications of the escrow exploitation mechanism are not yet final, either; they are considering the possibility of having the central site strip off the outer layers of encryption, and only sending the session key back to the decoder box.

The escrow authorities will NOT require presentation of a court order prior to releasing the keys. Instead, the agency will fill out a form certifying that they have a legal authorization. This is also backed up with a separate confirmation from the prosecutor's office. The escrow agencies will supply any key requested and will not themselves verify that the keys requested are associated with the particular court order.

As an aside, we've since been informed by a member of the civilian Skipjack review committee that the rationale for not having the escrow agency see the actual wiretap order is so that they do not have access to the mapping between key serial numbers and people/telephones.

Regarding the scale of the escrow exploitation system, they said that they did not yet have a final operational specification for the escrow protocols, but did say that the escrow agencies would be expected to deliver keys "~within about 2 hours~" and are aiming for "~close to real time.~" Initially, the FBI would have the decoder box, but eventually, depending on costs and demand, any law enforcement agency authorized to conduct wiretaps would be able to buy one. The two escrow agencies will be responsible for verifying the certification from and securely delivering the key halves to any such police department.

The NSA did not answer a question as to whether the national security community would obtain keys from the same escrow mechanism for their (legally authorized) intelligence gathering or whether some other mechanism would exist for them to get the keys.

The masks for the Clipper/Capstone chip are unclassified (but are protected by trade secret) and the chips can be produced in an unclassified foundry. Part of the programming in the secure vault includes "~installing part of the Skipjack algorithm.~" Later discussion indicated that the part of the algorithm installed in the secure vault are the "S-tables", suggesting that perhaps unprogrammed Clipper chips can be programmed to implement other 80-bit key, 32 round ciphers.

The Capstone chip includes an ARM-6 RISC processor that can be used for other things when no cryptographic functions are performed. In particular, it can be used by vendors as their own on-board processor. The I/O to the processor is shut off when a crypto operation is in progress.

They passed around a Tessera PCMCIA (type 1) card. These cards contain a Capstone chip and can be used by general purpose PC applications. The cards themselves might not be export controlled. (Unfortunately, they took the sample card back with them...) The card will digitally sign a challenge from the host, so you can't substitute a bogus card. The cards have non-volatile onboard storage for users' secret keys and for the public keys of a certifying authority.

They are building a library/API for Tessera, called Catapult, that will provide an interface suitable for many different applications. They have prototype email and ftp applications that already uses it. They intend to eventually give away source code for this library. They responded favorably to the suggestion that they put it up for anonymous ftp.

Applications (which can use the library and which the NSA approves for government use) will be responsible for managing the LEAF field. Note that they intend to apply key escrowed Skipjack to other applications, including mail and file encryption. The LEAF would be included in such places as the mail header or the file attributes. This implies that it is possible to omit sending the LEAF -- but the decrypt chip won't work right if it doesn't get one

When asked, they indicated that it might be possible wire up a pair of Clipper/Capstone chips to not transmit the LEAF field, but that the way to do this is "~not obvious from the interface we give you~" and "~you'd have to be careful not to make mistakes~". They gave a lot of attention to obvious ways to get around the LEAF.

The unit key is generated via Skipjack itself, from random seeds provided by the two escrow agencies (approximately monthly, though that isn't certain yet). They say they prefer a software generation process because its correct behavior is auditable.

Capstone (but not Clipper) could be configured to allow independent loading of the two key halves, in separate facilities. "~It's your money [meaning American taxpayers].~"

The LEAF field contains 80 bits for the traffic key, encrypted via the unit key in "~a unique mode <grin>~", 32 bits for the unit id, and a 16 bit checksum of some sort. (We didn't waste our breath asking what the checksum

algorithm was.) This is all encrypted under the family key using "~another mode <grin>~".

They expressed a great deal of willingness to make any sort of reasonable changes that vendors needed for their products. They are trying *very* hard to get Skipjack and key escrow into lots of products.

Finally, I should make clear that "Clipper" is more properly called the "MYK-78T".

[Matt, Thanks for the contribution, and thanks for making careful distinctions among the escrow initiative (EEI), the algorithm (Skipjack), the telephone implementation (Clipper), and the computer system/network implementation (Capstone). Much of what has been written on the subject has been confused because those distinctions were not consistently made. PGN]

Re: Campaign and Petition Against Clipper

Dorothy Denning <denning@cs.cosc.georgetown.edu> Wed, 09 Feb 1994 17:23:28 -0500 (EST)

CPSR has announced a petition campaign to oppose the Clipper initiative. I would like to caution people about signing the petition. The issues are extremely complex and difficult. The Clipper initiative is the result of considerable deliberation by many intelligent people who appreciate and understand the concerns that have been expressed and who worked hard to accommodate the conflicting interests. The decisions that have been made were not made lightly.

I would like to respond to some of the statements that CPSR has made about Clipper in their campaign and petition letters:

The Clipper proposal, developed in secret by the National Security Agency, is a technical standard that will make it easier for government agents to wiretap the emerging data highway.

The standard (FIPS 185) is not a standard for the Internet or any other high speed computer network. It is for the telephone system. Quoting from FIPS 185: "Data for purposes of this standard includes voice, facsimile and computer information communicated in a telephone system. A telephone system for purposes of this standard is limited to a system which is circuit switched and operating at data rates of standard commercial modems over analog voice circuits or which uses basic-rate ISDN or a similar grade wireless service."

The standard will not make it any easier to tap phones, let alone computer networks. All it will do is make it technically possible to decrypt communications that are encrypted with the standard, assuming the communications are not superencrypted with something else. Law enforcers still need to get a court order just to intercept the communications in the first place, and advances in technology have made interception itself more difficult. The standard will make it much

harder for anyone to conduct illegal taps, including the government.

The purpose of the standard is to provide a very strong encryption algorithm - something much stronger than DES - and to do so in a way that does not thwart law enforcement and national security objectives. Keys are escrowed so that if someone uses this technology, they cannot use it against national interests.

Industry groups, professional associations and civil liberties organizations have expressed almost unanimous opposition to the plan since it was first proposed in April 1993.

"The public does not like Clipper and will not accept it ..."

The private sector and the public have expressed nearly unanimous opposition to Clipper.

As near as I know, neither CPSR nor any other group has conducted any systematic poll of industry, professional societies, or the public. While many people have voiced opposition, there are many more organizations and people who have been silent on this issue. The ACM is in the process of conducting a study on encryption. CPSR is a member of the study group, as am I. Steve Kent is chair. Our goal is a report that will articulate the issues, not a public statement either for or against. The International Association for Cryptologic Research has not to my knowledge made any official statement about Clipper.

The Administration ignored the overwhelming opposition of the general public. When the Commerce Department solicited public comments on the proposal last fall, hundreds of people opposed the plan while only a few expressed support.

Hundreds of people is hardly overwhelming in a population of 250 million, especially when most of the letters were the same and came in through the net following a sample letter that was sent out.

The technical standard is subject to misuse and compromise. It would provide government agents with copies of the keys that protect electronic communications. "It is a nightmare for computer security."

I have been one of the reviewers of the standard. We have completed our review of the encryption algorithm, SKIPJACK, and concluded it was very strong. While we have not completed our review of the key escrow system, from what I have seen so far, I anticipate that it will provide an extremely high level of security for the escrowed keys.

The underlying technology was developed in secret by the NSA, an intelligence agency responsible for electronic eavesdropping, not privacy protection. Congressional investigations in the 1970s disclosed widespread NSA abuses, including the illegal interception of millions of cables sent by American citizens.

NSA is also responsible for the development of cryptographic codes to protect

the nation's most sensitive classified information. They have an excellent track record in conducting this mission. I do not believe that our requirements for protecting private information are greater than those for protecting classified information. I do not know the facts of the 1970s incident that is referred to here, but it sounds like it occurred before passage of the 1978 Foreign Intelligence Surveillance Act. This act requires intelligence agencies to get a court order in order to intercept communications of American citizens. I am not aware of any recent evidence that the NSA is engaging in illegal intercepts of Americans.

Computer security experts question the integrity of the technology. Clipper was developed in secret and its specifications are classified.

The 5 of us who reviewed the algorithm unanimously agreed that it was very strong. We will publish a final report when we complete or full evaluation. Nothing can be concluded from a statement questioning the technology by someone who has not seen it regardless of whether that person is an expert in security.

NSA overstepped its legal authority in developing the standard. A 1987 law explicitly limits the intelligence agency's power to set standards for the nation's communications network.

The 1987 Computer Security Act states that NIST "shall draw on the technical advice and assistance (including work products) of the National Security Agency."

There is no evidence to support law enforcement's claims that new technologies are hampering criminal investigations. CPSR recently forced the release of FBI documents that show no such problems.

CPSR obtained some documents from a few FBI field offices. Those offices reported no problems. CPSR did not get reports from all field offices and did not get reports from local law enforcement agencies. I can tell you that it is a fact that new communications technologies, including encryption, have hampered criminal investigations. I personally commend law enforcement for trying to get out in front of this problem.

If the plan goes forward, commercial firms that hope to develop new products will face extensive government obstacles. Cryptographers who wish to develop new privacy enhancing technologies will be discouraged.

The standard is voluntary -- even for the government.

Mr. Rotenberg said "We want the public to understand the full implications of this plan. Today it is only a few experts and industry groups that understand the proposal.

I support this objective. Unfortunately, it is not possible for most of us to be fully informed of the national security implications of uncontrolled encryption. For very legitimate reasons, these cannot be fully discussed and

debated in a public forum. It is even difficult to talk about the full implications of encryption on law enforcement. This is why it is important that the President and Vice-President be fully informed on all the issues, and for the decisions to be made at that level. The Feb. 4 decision was made following an inter-agency policy review, headed by the National Security Council, that examined these issues using considerable input from industry, CPSR, EFF, and individuals as well as from law enforcement and intelligence agencies. In the absence of understanding the national security issues, I believe we need to exercise some caution in believing that we can understand the full implications of encryption on society.

As part of the Feb. 4 announcement, the Administration announced the establishment of an Interagency Working Group on Encryption and Telecommunications, chaired by the White House Office of Science and Technology Policy and National Security Council, with representatives from Commerce, Justice, State, Treasury, FBI, NSA, OMB, and the National Economic Council. The group is to work with industry and public interest groups to develop new encryption technologies and to review and refine encryption policy. The NRC's Computer Science and Telecommunications Board will also be conducting a study of encryption policy.

These comments may be distributed.

Dorothy Denning, Georgetown University



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 49

Thursday 10 February 1994

Contents

FireFly in the ointment?

Don Watts

Aging software ages suddenly!

Don Watts

Clinical diagnosticians and diagnostic clinicians

David Honig

UK bank preparing for electronic money trial

John Grav

What goes around, comes around

Paul Robinson

Electronic rumours

Mich Kabay

Medicare Transaction System & the Electronic Superhighway

Mich Kabay

Re: Risks of cliche collisions on the information superhighway

Mark Jackson

Re: White House documents

Bill Casti via David Crawford

Re: Cantwell and Spoofed Representatives?

Jon Leech

Re: Sounding the Alarm

Robert J Horn

Re: Verify your backups

Timothy Miller

Dan Lanciani

Martin Minow

EMI article in IEEE Spectrum

Robert J Horn

Information on RISKS

comp.risks

Info on RISKS (comp.risks)

FireFly in the ointment?

"Peter G. Neumann" < neumann@chiron.csl.sri.com> Thu, 10 Feb 1994 10:57:13 PST

Don Watts of Tustin CA checked in by SnailMail with a note that the StarWars decoy/laser-radar program (FireFly) worked completely backwards (for example, with respect to incoming maneuvers) because the accelerometer was wired in opposition to the directional assumption in the software. (The shaker tests of the decoy were omitted in an effort to save money.)

✓ Aging software ages suddenly!

"Peter G. Neumann" < neumann@chiron.csl.sri.com> Thu, 10 Feb 1994 10:57:13 PST

Don Watts also offered the following memo from Steven Ray of the Ball Efratom Division, dated 20 Jan 1994, and lightly edited by PGN.

Aging Analysis Software malfunction

On Monday, 17 January 1994, a 'bug' developed in the IBM-based 'Ball Aging Analysis' software program. This bug prevents us from plotting any aging data after 16 Jan 1994 even though the data actually exists in the database. This bug effectively shut down all shipments of units because no graphs could be generated. After some initial investigation, this bug was linked to the modified Julian date of 2148 and that any date before that was OK, but any data after that would not plot. So, as a temporary fix while the software code is being corrected and to continue to be able to ship units, I have set the dates on all of the Aging computers back one year, to 1993, so that the aging data can be plotted on all Aging plots until a permanent fix can be done.

Clinical diagnosticians and diagnostic clinicians

David Honig <honig@ruffles.ICS.UCI.EDU> Tue, 08 Feb 1994 14:03:07 -0800

Which of the following is *not* a reason for the clinician to remain an essential part of the diagnostic process?

- A Computers are unable to collect and evaluate nonverbal data.
- B Patients have poor acceptance of computer-assisted assessment.
- C Computers are poor at temporal reasoning.
- D Computers cannot assess the clinical significance of a behavior.

The answer was given as B, though of course AI researchers are working on the others....

Anyway, the _Psychiatric Annals_ Jan 1994 Vol 24, No 1 issue is about "Using Computers in Psychiatry". Shrinks can get continuing education credit for reading this mag and mailing in a quiz included.

Titles of articles range from using computers to teach ugrads (including showing video clips of psychopaths from popular hollywood productions..) to expert systems making drug recommendations, to computational models of the mind and Psychiatry. Most articles are written by MDs with a few real doctorates.

UK bank preparing for electronic money trial

John Gray <grayjw@cs.aston.ac.uk> Tue, 8 Feb 94 13:42:41 GMT

I was hoping that someone else might have seen more about this and posted information here, but it appears not; in that case I'll mention what I know, in the hope that someone will be able to fill in the details.

One of the big UK banks is apparently planning to introduce a trial in Swindon, UK of an electronic money system, where money is held on plastic cards (I'm not sure whether magnetic or smart). Money is transferred through the system using either a handheld reader or an EFTPOS system in a shop. The cards are not personal, but can be locked with a 4-digit PIN code. A card that isn't locked can be used by anyone, while a locked card requires the code in order to view the balance or deduct money from the card. The nature of the system allows individuals to transfer money from card to card using the appropriate palmtop-sized system.

I assume that the money is "cryptographic", but I've forgotten the details (I read all this in a paper some months agp). Does anyone know any more about this system? It raises a whole host of issues, both social and technical.

John Gray

What goes around, comes around

Paul Robinson <PAUL@TDR.COM> Sun, 6 Feb 1994 01:17:49 -0500 (EST)

The following was posted on a local BBS about the recent incident on the network.

ANDREWS NEWS

Staff member suspended for network abuse, by Wendy Wein

Clarence Thomas, systems administrator for "Redwood," the administrative computer, will be temporarily suspended from his job because he sent a 5,500 character religious message to between 1,200 to 1,500 news groups across the world through the Internet. This act violated the system's purpose, giving Andrews University a bad reputation among the Internet users. Over 1,200 complaints came over the Internet to the Andrews computer science department demanding justice.

According to Mailen Kootsey, chair of the academic computing committee

and dean of the College of Arts and Sciences, Thomas will be suspended from his position for a week. His status will be reviewed at the end of the time period. During this week Thomas will not have available access to the network computers.

Sometime between five and eight o'clock Monday evening, January 17, Thomas sent his three-page message titled "Global Alert for All: Jesus is Coming Soon," from the Andrews computing center to the news groups which are accessible through the Internet, a computer system which connects computers throughout the world.

These news groups deal with different individual topics. For example, if a news group is about cars, then only information about cars should be sent to that news group. Some people subscribe to more than one group and some universities and organizations are subscribed to almost all of them. Thomas sent his religious message to all of these groups.

People who were not interested received this message, some more than once. Some organizations received 1,200 to 1,500 copies. For many of the subscribers religious input was not accepted very well. This message took up their time and money. The message accumulated 5.5 kilobytes of disk space. Within an hour after the message was sent, Daniel Bidwell, administrative contact for the network at Andrews, received Internet messages from the East coast.

In two hours they came from the West coast and within four hours, complaint letters came in from other countries. The letters made statements such as "This is not what I am paying for" and "Will this guy be stopped?"

In addition to the news groups, Thomas also sent his message through a mailing list, filling others' electronic mail. This could have been changed by sending it to only a few news groups so fewer copies could have been distributed. "If he sent his message through a news group which dealt with religious issues then everything would be fine," said Bidwell, "No one would have known."

There are no laws against Thomas' actions, yet he violated and broke some of the unwritten rules of society. That is why many people are unhappy.

This act created poor reactions towards the university. Thomas' intent was to spread the good news of Jesus' return to all those he could reach. Thomas was trying to witness to others, yet instead of creating joy in peoples' heart, he only created anger and resentment. "He was doing the right thing in the wrong way," said Bidwell.

Some of those who wrote to complain said that they agreed with the message, but that Thomas delivered it wrongly. This message has created bad public relations for the church at another's expense.

The letters that were received included threats. They wanted Thomas fired, or else the Internet connections from the Andrews campus could be "taken." People are now writing and finding ways to contact President Lesher. Not only have strangers called, but also a large amount of Adventists claiming that something must be done to save the church's sacred reputation.

On Monday morning, January 24, Rob Barnhurst, Thomas's supervisor and director of the computing center, Ed Wines, vice president for finance, and Kootsey, met to discuss the incident. They decided to send out an apology through the Internet, explaining that they did not condone Thomas's act and will try to keep this from happening again.

Thomas graduated from Andrews with a computer science degree. Those at the computer science department feel that he knew better then to send out that many copies. "It was clearly, very definitely abuse," said Ray Paden, chair of the computer science department. "He broke the guidelines for the Internet

and violated the net etiquette. The trust was violated."

Electronic rumours

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 05 Feb 94 22:30:12 EST

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

Glitch Reveals The Power Of Internet; New Group's Offer Unleashes Users' Tirade By John Burgess and John Schwartz, Washington Post Staff Writers, 31 Jan 1994

A small organization promising free access to a global computer network found itself recently the focus of a deluge of electronic hate mail. To its chagrin, the messages were carried all over the world by the very network the group promotes, the Internet.

The authors explain that the International Internet Association (IIA) issued ads last year offering free access to the Internet. However, to get access, eager users had to submit a credit card number. Then, potential customers were told, the free-access ports were generally busy. If they wished, such customers could subscribe to the service at \$0.20/minute, charged to the credit card.

Scott Ward, an official with CapAccess of Washington, DC, another service providing free Internet access, investigated IIA and couldn't locate any evidence of its computer. He then sent out an electronic warning that was widely circulated. He wrote, "I am not convinced this organization exists and highly discourage any Internet user from sending information until you make certain that the IIA is real."

Unfortunately for everyone involved, the IIA was real. The Executive Director of the IIA, Max Robbins, promised to repair the damage to its credibility caused by the incorrect electronic rumour. He announced changes in the organization's financing: all access would be free, but the IIA would solicit corporate donations.

This story once again illustrates the need for the same (or greater) level of care in verifying what we post on the Internet. Because information in electronic form doesn't fade, get wrinkled, or impossible to read after multiple use, electronic rumours can circulate forever. RISKS readers will recall the case of Craig Shergold's unstoppable avalanche of post cards.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Medicare Transaction System & the Electronic Superhighway

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM>

30 Jan 94 14:53:24 EST

>From the Washington Post newswire via Executive News Service (GO ENS) on CompuServe:

Medicare Billing to Join Electronic Superhighway; One National System to Handle All Payments, By Spencer Rich, Washington Post, 20 Jan 1994

By the end of the decade, one giant nationwide computer system will electronically pay nearly all of the 1 billion bills Medicare handles each year. Beneficiaries will only have to hand their Medicare cards to their doctors, hospitals, laboratories or nursing homes to make sure their bills get paid.

Once a patient's identification number is punched into a terminal at a hospital or doctor's office, the computer will compute how much Medicare owes, electronically transfer that amount to the doctor's or hospital's bank account, calculate how much an individual's Medigap (supplemental insurance) policy owes and automatically bill for that. If the Medicare beneficiary has no Medigap policy, the government computer will bill the patient for whatever is owed."

The article continues with the following key points:

- o \$19 million six-year contract to GTE Government Systems Corp. of Chantilly, Va., for design and implementation;
- o implementation '96-'98;
- o Medicare Transaction System (MTS) will eliminate many manual procedures;
- o may save \$200 million a year.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

[Maybe it is time for the MediBempsters to write a song about healthcare along the superhighway. PGN]

Re: Risks of cliche collisions on the information superhighway

Mark Jackson <MJackson.wbst147@xerox.com> Mon, 7 Feb 1994 13:09:12 PST

As an addendum to Phil Agre's note in Risks 15.44, PGN begins:

- > [We are going to see all sorts of metaphors springing up on the
- > InfoSuperhighway, such as. . .

Perhaps most evocative, from the "Editor's Note" on the state and future of journalism in the January/February issue of the /Columbia Journalism Review/:

Only now, thanks to the new technology, the public doesn't have to take it anymore; with every passing day people have more alternatives to the traditional news media to choose from, a situation that has prompted commentator Jeff Greenfield to warn that journalists may become "roadkill on the information highway."

Mark Jackson

★ Re: White House documents (from alt.internet.services)

Wed, 9 Feb 94 16:15 PST

Article 13945 of alt.internet.services:

Path: vortex.com!rand.org!usc!howland.reston.ans.net!news.intercon.com!vector.casti.com!quire

From: quire@vector.casti.com (Bill Casti)

Newsgroups: alt.internet.services

Subject: Re: Altered White House documents

Date: 9 Feb 1994 21:53:21 GMT

Organization: The Gnomes of Zurich (shhh!)

Chris Fulmer (chrisf@brtph316.bnr.ca) wrote:

: At the risk of extending this to the point that it should go elsewhere...

: I believe that the original post said that the on-line version of the

: remarks differed from the remarks that were actually stated. While the

: President's position may have changed, the remarks that he made certainly

: didn't.

re: "revised documents on ftp server".....

----- Forwarded message -----

Date: Mon, 07 Feb 1994 16:29:29 -0700 (MST)

From: crawford@fido.econlab.arizona.edu (David W. Crawford)
Subject: Revised Documents on FTP server without version number

>From croberts@crl.com Mon Feb 7 09:47:09 1994

>Newsgroups: alt.internet.services

>Subject: Altered White House documents

>Date: 5 Feb 1994 09:38:23 -0800

>

>I assume everyone knows about the ftp site whitehouse.gov. I just >discovered that the Clinton rebuttal to Elizabeth McCaughey's

>critique of his health care plan has been altered on

>whitehouse.gov - with no mention in the current version that it

>has been changed.

I assume that neither of you know the difference between a speech-as-written and a speech-as-delivered.

>According to Associated Press writer Tom Raum, the original White >House rebuttal to McCaughey's New Republic magazine article used >the word "lie" four times. The copy of the White House rebuttal I >just downloaded (Feb 5, morning, pacific time) does not contain >the word lie nor does it contain any indication that it is a >"revised" version.

Then, it's the speech-as-written and not the speech-as-delivered.

>White House spokesman Dee Dee Myers defended the rebuttal on >Thursday although she conceded that "perhaps the language was a >little strong." Clinton, asked by reporters earlier this week >about calling McCaughey's comments lies, responded, "Well, I hate >to use that word, but the New Republic article was way off base >and the New Republic didn't make total disclosure about the source >of the article." So Clinton admitted to the use of "lie" but it >has since been removed from the version available for anonymous >ftp at whitehouse.gov. Makes you wonder just how self- serving and >accurate the rest of the information there might be...

That's a knee-jerk reaction and totally inaccurate. The speeches-as-written are usually delivered a few hours in advance of the speech, with an embargo on publication until the speech has been delivered (the same embargo the rest of the news media observes, by the way). If you look in the White House Papers gopher hole (accessible for anonymous ftp by telnetting to vector.casti.com), which mirrors the gopher SUNsite at Syracuse University), there are several examples of speeches-as-written (indicated by "as prepared") being followed by clearly indicated "CORRECTED--as delivered" speeches.

>UWSA'ers note: the whitehouse.gov directory /pub/political->science/speeches/perot contains the text of Perot's book "United >We Stand," and various Perot speeches. But no, I have not double->checked them for unauthorized "revisions."

These are no longer contained in directories which are mirrored by whitehouse.gov, as they are not White House documents. Talk to Mr. Perot and get the address of *his* ftp site (I doubt if he has one).

In the future, make sure you get the FACTS before you spout off about stuff you--apparently--know nothing about. I know that doing a bit of investigative research would greatly hobble your arguments, but it would be the courteous thing to do.

If you have questions about what is or isn't contained in the documents available through whitehouse.gov, ask first.

The address for comments/questions/suggestions about the document site is:

publications-comments@whitehouse.gov

Bill Casti

Re: Cantwell and Spoofed Representatives?

Jon Leech <leech@cs.unc.edu> 9 Feb 1994 19:23:16 -0500

In <u>RISKS-15.47</u>, mech@eff.org (Stanton McCandlish) asks us to "*Please take a moment to send e-mail to U.S. Rep. Maria Cantwell (cantwell@eff.org) to show your support of H.R. 3627, her bill to liberalize export controls on encryption software.*" Later, he writes "EFF will deliver printouts of all letters to Rep. Cantwell."

It's unclear if Rep. Cantwell

- (a) asked for the account to be established,
- (b) was aware of the account's existence, or
- (c) had no idea of the existence of the account (though I'm sure she does by now :-)

If EFF is acting on its own initiative as a mail to print reflector for Rep. Cantwell, perhaps this should be stated and some other, non-confusing name used for the mail drop? I would think EFF needs to be particularly careful to avoid confusion on details like this...

Jon Leech (leech@cs.unc.edu) UNC Pixel-Flow Project

Re: Sounding the Alarm

Robert J Horn <rjh@world.std.com> Wed, 9 Feb 1994 20:37:42 -0500 (EST)

- > "driving doctors and nurses to distraction" who agree that "alarm noise
- > pollution is a significant problem that threatens patient health"
- > presumably because "doctors order that all alarms be disconnected except
- > those deemed absolutely necessary for patient safety."

For more information and detail on one aspect of this see the December 1993 issue of IEEE Engineering in Medicine and Biology. This magazine is probably of interest to many Risks readers, since the subject is an intersection of a significant risk area with a significant computer content.

The discussion of ethics in the December issue is probably the most important. It should act as a strong reminder that the risk of computer malfunction is merely one aspect of system ethical analysis. Just as most people now understand that risk analysis must include the whole operational environment, not just the literal instructions, we will eventually learn to consider risks in the larger ethical context. The initial step is to begin to understand the ethical issues.

Rob Horn horn@temerity.polaroid.com

★ Re: Verify your backups (Heberlein, RISKS-15.39)

Timothy Miller <tsm@cs.brown.edu>

Sun, 23 Jan 94 14:56:02 -0500

Isn't wuarchive one of the more widely mirrored archive sites? Couldn't they get most of their files back by copying from the mirrors? I know this misses the original point about failed backups as far as other sites are concerned, but it seems to me there are benefits of as well as risks from computers and technology here. Tim

★ Re: Bad backups (really NEC CD-ROM problem) (Hamlet, RISKS-15.43)

Dan Lanciani <ddl@das.harvard.edu> Sun, 30 Jan 94 19:17:59 EST

> ... the FORTRAN library disk i-o routine did retry for read failure,

This reminds me of something I had meant to send in long ago, but which may still be relevant. The NEC CDR-72 CD-ROM seems to have used a similar, highly successful error recovery technique. I don't remember the exact details, but the drive would substitute either the previous or the next block for the one it had meant to retry. There was absolutely no indication of error to the host machine, just _silent_ data corruption. Given what we expect from CD-ROMs, the risks of this kind of failure mode are obvious. (Oh, and note that this problem showed up with the first soft errors after but a few months of dust accumulation.)

I think NEC's treatment of the problem shows a worse risk, though. They knew the flaw existed and they took no action to contact registered owners (let alone unregistered ones). Moreover, their first-level technical support was either uninformed or else was instructed to avoid the issue. When I explained the problem to them in great detail, they kept insisting that I send them the specific CD that was showing the problem and/or try a different CD in the drive. They could not (or would not) grasp the concept that an unreported error was unacceptable in this context. And they felt that if any CD could be found to read without corruption at least once then the drive must be fine. I asked that they have somebody with a more technical background get back to me, and indeed somebody did get back to me.

The technical person was so technical, of course, that he would not listen to my detailed description of which blocks ended up where. Instead he required me to bring the phone to the computer to perform a "special test." The test turned out to be to copy a file from the CD to the hard disk and then run the "special" DOS program COMP on the two copies. I was to report the number of mismatches shown. The number of mismatches was the maximum that COMP will display before giving up, and reciting that number won me a replacement drive for what he admitted was a known problem. I hate to think what would have happened if the drive failed the same way during the COMP as during the copy. Or worse, if I didn't have a DOS machine on which to run the "special test" to his satisfaction.

I'm no expert on the uses of CD-ROMs, but I'll bet someone can come up with a pretty bad scenario caused by these kinds of errors.

Dan Lanciani ddl@harvard.*

✓ re: backups (Hamlet, RISKS-15.43)

Martin Minow <minow@apple.com> Mon, 7 Feb 94 13:45:37 -0800

In Risks 15.43, Dick Hamlet wrote:

- > How many dump systems today read back what has been written for backup
- > (much less check it or do a file compare!) unless there is a restore request?

This is a normal option to Retrospect, a backup package for Macintosh. It seems to work very well.

Martin Minow minow@apple.com

EMI article in IEEE Spectrum

rob horn <horn%temerity@leia.polaroid.com> 07 Feb 1994 15:23:36 -0500 (EST)

There is a good summary article on EMI/EMC in aircraft in the current issue of IEEE Spectrum. Not much new to RISKs readers, but a good overview of the present situation.

Rob Horn horn@temerity.polaroid.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 50

Thursday 10 February 1994

Contents

Re: Dorothy Denning's contribution to RISKS-15.48 on EES/Clipper/etc.

Barbara Simons

Marc Rotenberg

George T. Talbot

Lance J. Hoffman

Fredrick B. Cohen

A. Padgett Peterson

Geoff Kuenning

Info on RISKS (comp.risks)

★ Re: Campaign and Petition Against Clipper (Denning, RISKS-15.48)

"Barbara Simons" <simons@vnet.IBM.COM> Thu, 10 Feb 94 13:48:52 PST

In RISKS-15.48, 9 Feb 1994, Dorothy Denning states:

>As near as I know, neither CPSR nor any other group has conducted any >systematic poll of industry, professional societies, or the public. While >many people have voiced opposition, there are many more organizations and >people who have been silent on this issue. The ACM is in the process of >conducting a study on encryption. CPSR is a member of the study group, as am >I. Steve Kent is chair. Our goal is a report that will articulate the >issues, not a public statement either for or against. The International >Association for Cryptologic Research has not to my knowledge made any official >statement about Clipper.

I am chair of USACM, which is the new U.S. Public Policy Committee of ACM. A few months ago we asked Steve Kent to chair a panel that would study encryption policy in the U.S. and produce a report for ACM. As Dorothy mentions, she is on the panel, together with several other illustrious individuals, including the esteemed moderator of RISKS. I have included the list of panelists at the end of this note. CPSR is no more a member of the panel than are the National Security Agency or the Department of Justice.

The panel does have members who are affiliated with all three organizations.

I am certain that Dorothy did not intend to give the impression that the ACM panel has decided that ACM will not have a public position on Clipper. However, since her email might have been misinterpreted by some readers, I want to clarify that, while ACM has not taken a position on Clipper, there has not been any decision made within ACM of which I am aware that prevents ACM from taking a position at some future time. In addition, it is my understanding that there has been no final determination made by the panel of precisely what the report will or will not contain.

Barbara Simons, Chair USACM

The members of the ACM encryption policy panel are:

Dr. Clint Brooks, National Security Agency

Scott Charney, Department of Justice

Dr. Dorothy Denning, Georgetown University

Dr. Whitfield Diffie, Sun Microsystems Inc.

Dr. Anthony Lauck, Digital Equipment Corporation

Douglas Miller, Software Publishers Association

Dr. Peter Neumann, SRI International

Dave Sobel, Computer Professionals for Social Responsibility

Chair: Dr. Stephen Kent, Bolt Beranek & Newman Staff: Dr. Susan Landau, University of Massachusetts

Re: CPSR Clipper Campaign

Marc Rotenberg <Marc_Rotenberg@washofc.cpsr.org> Thu, 10 Feb 1994 16:07:13 EST

Dorothy Denning has raised important questions about the Clipper proposal. As she says "the issues are extremely complex and difficult." Below I've tried to answer the points she has raised. I apologize in advance to RISKS readers who know all of this.

Please read her comments and my response. Speak with others interested in the Clipper proposal. If on balance, after reviewing the arguments, you decide Clipper is a mistake then you should express your opposition by sending a message to:

CLIPPER.PETITION@CPSR.ORG

with the words

"I oppose Clipper"

in the subject header. If you have already signed the petition, ask a friend or colleague to sign.

Your help is needed.

Marc Rotenberg, director, CPSR Washington office

- <> The Clipper proposal, developed in secret by the
- <> National Security Agency, is a technical standard
- <> that will make it easier for government agents to
- <> wiretap the emerging data highway.
- > The standard (FIPS 185) is not a standard for the
- > Internet or any other high speed computer network. It
- > is for the telephone system.

The letter to the President makes clear that we are concerned about "Clipper and associated standards" which include the Capstone EES configuration for data transmission.

It is clearly the intent of the EES proposal to cover both voice and data transmissions.

- > The standard will not make it any easier to tap phones,
- > let alone computer networks. All it will do is make it
- > technically possible to decrypt communications that are
- > encrypted with the standard, assuming the communications
- > are not superencrypted with something else.

This is a little bit like saying that leaving a master key for every house on your block with the police will not make it easier for the police to open locked doors.

We may disagree about whether this is a good idea, but let's be clear about the intent of the proposal.

- > The purpose of the standard is to provide a very strong
- > encryption algorithm something much stronger than DES
- > and to do so in a way that does not thwart law
- > enforcement and national security objectives. Keys are
- > escrowed so that if someone uses this technology, they
- > cannot use it against national interests.

The NSA is responsible for foreign signal interception. It has no legal authority to conduct wire surveillance. What are the NSA's "national security" interests in domestic wire surveillance?

- <> Industry groups, professional associations and
- <> civil liberties organizations have expressed almost
- <> unanimous opposition to the plan since it was first
- <> proposed in April 1993.
- <> The private sector and the public have expressed
- <> nearly unanimous opposition to Clipper.
- > As near as I know, neither CPSR nor any other group has
- > conducted any systematic poll of industry, professional
- > societies, or the public.

To the best of my knowledge, there has never been a proposed technical standard that generated more opposition. Firms across the telecommunications and computer industry oppose Clipper. Computer security people and cryptographers oppose Clipper. Privacy experts oppose Clipper.

- <> The Administration ignored the overwhelming
- <> opposition of the general public. When the Commerce
- <> Department solicited public comments on the
- <> proposal last fall, hundreds of people opposed the
- > plan while only a few expressed support.
- > Hundreds of people is hardly overwhelming in a
- > population of 250 million, especially when most of the
- > letters were the same and came in through the net
- > following a sample letter that was sent out.

I would encourage Dorothy, or anyone else, to take a poll of any representative user group -- RISKS readers perhaps -- if there is any doubt about how the public feels about the proposal.

- <> The technical standard is subject to misuse and
- <> compromise. It would provide government agents with
- <> copies of the keys that protect electronic
- <> communications. "It is a nightmare for computer
- <> security."
- > I have been one of the reviewers of the standard. We
- > have completed our review of the encryption algorithm,
- > SKIPJACK, and concluded it was very strong. While we
- > have not completed our review of the key escrow system,
- > from what I have seen so far, I anticipate that it will
- > provide an extremely high level of security for the
- > escrowed keys.

Dorothy endorsed the proposal before she joined the "review" team. The group that she refers to, a White House task force, has an interesting history. The majority of cryptographers asked to participate declined.

- <> The underlying technology was developed in secret
- <> by the NSA, an intelligence agency responsible for
- <> electronic eavesdropping, not privacy protection.
- <> Congressional investigations in the 1970s disclosed
- <> widespread NSA abuses, including the illegal
- <> interception of millions of cables sent by American
- <> citizens.
- > NSA is also responsible for the development of
- > cryptographic codes to protect the nation's most
- > sensitive classified information. They have an
- > excellent track record in conducting this mission.

Senator Frank Church, who conducted the most extensive hearings ever held on

the National Security Agency, said that the NSA's intelligence gathering capabilities were important for the security of the United States. He also said that the massive eavesdropping capability created "A tremendous potential for abuse." If ever turned against the communications system of the United States:

no American would have any privacy left . . . there would be no place to hide.

We must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is an abyss from which there is no return. " (NBC Meet the Press, 1975)

- <> Computer security experts question the integrity of
- <> the technology. Clipper was developed in secret and
- <> its specifications are classified.
- > The 5 of us who reviewed the algorithm unanimously
- > agreed that it was very strong. We will publish a final
- > report when we complete or full evaluation. Nothing can
- > be concluded from a statement questioning the technology
- > by someone who has not seen it regardless of whether
- > that person is an expert in security.

The original CPSR letter to the President, asking for the withdrawal of Clipper, was signed by Hellman, Rivest, Diffie, Merkle, and others. Many more experts are adding their names daily to the CPSR petition.

- <> NSA overstepped its legal authority in developing
- <> the standard. A 1987 law explicitly limits the
- <> intelligence agency's power to set standards for
- <> the nation's communications network.
- > The 1987 Computer Security Act states that NIST "shall
- > draw on the technical advice and assistance (including
- > work products) of the National Security Agency."

The original replacement for DES, proposed by the Department of Commerce in 1989, would have had these characteristics:

- -- public, unclassified
- -- implementable in both hardware or software
- -- usable by federal Agencies and U.S. based multi-national corporation
- -- a level of security sufficient for the protection of unclassified, sensitive information and commercial propriety and/or valuable information.

The final proposal, developed with the "technical assistance" of the NSA, has these characteristics.

- -- The Clipper algorithm Skipjack is classified
- -- Public access to the reasons underlying the proposal is restricted
- -- Skipjack can be implemented only in tamper-proof hardware

- -- It will not be used by multi-national corporations
- -- The security of the configuration remains unproven.

The Computer Security Act was passed precisely because the NSA tried previously to grab civilian computer security turf. The law was specifically intended to control the type of abuse that results from secret standard-setting arrangements.

If there any doubt among RISKS readers about the illegal activities of the NSA in the development of the EES, please consult the minutes of the NSA/NIST Technical Working Group (TWG) that produced the standard. The minutes should be available from the National Security Agency Public Information Office. That phone number is 301/688-6524.

- <> There is no evidence to support law enforcement's
- <> claims that new technologies are hampering criminal
- <> investigations. CPSR recently forced the release of
- <> FBI documents that show no such problems.
- > CPSR obtained some documents from a few FBI field
- > offices. Those offices reported no problems. CPSR did
- > not get reports from all field offices and did not get
- > reports from local law enforcement agencies. I can tell
- > you that it is a fact that new communications
- > technologies, including encryption, have hampered
- > criminal investigations.

The statement is illogical. There is still no evidence to support the FBI's claims.

The FBI made certain claims that cryptography was impeding criminal investigation conducted by wiretap. CPSR investigated the FBI's claims by filing a Freedom of Information Act suit to obtain the relevant documents. The documents provided to us by the Department of Justice revealed that none of the FBI field officers had encountered any obstacles. The Department of Justice has just informed us that they provided to us all relevant documents concerning the Clipper proposal.

There is one reported case where cryptography made it difficult for law enforcement to obtain evidence. That case concerned reading the contents of a file on a hard disk after it was seized.

If this is the problem that the Clipper proposal is intended to solve, then the key escrow scheme must be extended to every single encrypted file -- not just encrypted communications -- everywhere in the world.

Every encrypted file. Everywhere.

- <> If the plan goes forward, commercial firms that
- <> hope to develop new products will face extensive
- <> government obstacles. Cryptographers who wish to
- <> develop new privacy enhancing technologies will be
- <> discouraged.

> The standard is voluntary -- even for the government.

An FBI legislative proposal now under consideration at the White House would mandate a Clipper-like scheme. That proposal is backed by fines up to \$10,000 per day and jail time.

That's not voluntary.

- <> Mr. Rotenberg said "We want the public to
- <> understand the full implications of this plan.
- <> Today it is only a few experts and industry groups
- <> that understand the proposal.
- > I support this objective. Unfortunately, it is not
- > possible for most of us to be fully informed of the
- > national security implications of uncontrolled
- > encryption. For very legitimate reasons, these cannot
- > be fully discussed and debated in a public forum.

This assertion has never been supported by evidence. It has been used simply to stifle criticism.

- > The Feb. 4 decision was made
- > following an inter-agency policy review, headed by the
- > National Security Council, that examined these issues
- > using considerable input from industry, CPSR, EFF, and
- > individuals as well as from law enforcement and
- > intell

CPSR did not participate in the inter-agency policy review. Our position from the very beginning is that these decisions must be made openly.

- > In the absence of understanding
- > the national security issues, I believe we need to
- > exercise some caution in believing that we can
- > understand the full implications of encryption on
- > society.

This premise, if accepted, would mean that people in the United States would have no right to express political views when the government claimed "national security." Certainly, there are matters of national security that must be protected, but when an agency with expertise in wire surveillance develops a secret standard for eavesdropping and tells those who raise questions that there are matters of national security that they would not understand, there is good reason for concern.

If you believe that Clipper is a mistake, please express your views by sending email with the words "I oppose Clipper" in the subject header to CLIPPER.PETITION@CPSR.ORG.

[In the following messages, I have pruned back radically on the included repetitions of Dorothy's original message. I hope I have not lost any threads... Refer back to <u>RISKS-15.48</u> if you are in doubt. PGN]

Re: Campaign and Petition Against Clipper

George T. "14K F/D" Talbot <ugtalbot@king.mcs.drexel.edu> Wed, 9 Feb 94 22:16:51 EST

I would like to comment upon a few points raised by Dr. Denning:

>The decisions that have been made were not made lightly.

While I appreciate the sentiments expressed by Dr. Denning here, I'm sure that those who oppose the Clipper initiative are also intelligent and have also worked very hard to make their concerns known. I have studied this issue actively and I assure you that I did not sign the petition "lightly".

>The standard (FIPS 185) is not a standard for the Internet or any other high >speed computer network.

While the Clipper initiative only covers the phone system, the entire proposal (Clipper and Capstone and the key escrow system) will touch the high-speed networks and should be taken as a whole.

>...assuming

>the communications are not superencrypted with something else. Law >enforcers still need to get a court order just to intercept the >communications in the first place...

There are two points to address here. First, it is currently very difficult to produce and export cryptographic software of any significant strength due to export controls. A private entity which has the resources to produce a strong cryptographic solution will have to invest a great deal to produce such software. The current export controls would make it impossible for such an entity to compete on the world market, thus limiting profit, possibly to the point of non-profitability. This makes superencryption pretty unlikely, and this is one of the purposes of the current export controls on encryption. Also at issue is whether the government will outlaw non-Clipper/Capstone/Key Escrow encryption entirely.

Second, law enforcement needs to get a court order to intercept phone communications. I know of no such need to get a court order to intercept communications on a high speed network w.r.t. Capstone. The current administration proposal does not require a court order to get the escrowed keys themselves.

- > The Administration ignored the overwhelming opposition of the
- > general public. When the Commerce Department solicited public
- > comments on the proposal last fall, hundreds of people opposed the
- > plan while only a few expressed support.

>

>Hundreds of people is hardly overwhelming in a population of 250 million, >especially when most of the letters were the same and came in through the net >following a sample letter that was sent out.

Currently the community which is informed on this issue is rather small. It is unclear whether that population of 250 million would support the initiative if they were fully informed. Assuming the people which responded to the Commerce Department solicitation is representative of the public at large, it is clear that this is not a popular initiative outside of government/law enforcement/national security circles.

>I have been one of the reviewers of the standard. We have completed our >review of the encryption algorithm, SKIPJACK, and concluded it was very >strong. While we have not completed our review of the key escrow system, from >what I have seen so far, I anticipate that it will provide an extremely high >level of security for the escrowed keys.

I'm sure that the committee which reviewed the algorithm made as accurate an assessment of the algorithm they could in the limited time they were given. What the NSA refuses to answer on this point is whether it, or the rest of the national security community will use the escrow system. If the [national security] community does not sign up [for the key escrow system], then the escrow system will be effectively compromised.

>...I am not aware of any recent evidence >that the NSA is engaging in illegal intercepts of Americans...

From what I understand, the Act was passed in response to the incident in the 1970s. Just because one doesn't have evidence doesn't mean that abuses don't exist, and one can't make basic policy decisions based upon that. When considering important policy like this, one has to actively consider the risks of abuse.

>...

From what current reports show, NSA pushed the proposal through NIST, and it was NSA, not NIST, which was the true author and sponsor of the initiative. They were operating on a "gray area" where because they were the only source for the standard considered, they effectively set the standard without explicitly violating the law.

>... I can tell you that it

>is a fact that new communications technologies, including encryption, have >hampered criminal investigations. I personally commend law enforcement for >trying to get out in front of this problem.

Dr. Denning, would you, as a service to RISKS readers, disclose your evidence of how encryption has hampered criminal investigations? And how often? And what kind of investigations were hampered?

In the absence of understanding the national security issues, Ibelieve we need to exercise some caution in believing that we can understandthe full implications of encryption on society.

I disagree and Dr. Denning contradicts herself. If the decision is made at those levels, the public will not be informed. This policy is too important to relegate to a back room.

George T. Talbot

Clipper standard came close to being not only for phones

"Lance J. Hoffman" <hoffman@seas.gwu.edu> Thu, 10 Feb 1994 08:28:46 -0500 (EST)

Dorothy Denning wrote in RISKS Forum:

- > The [Clipper] standard (FIPS 185) is not a standard for the Internet or any
- > other high speed computer network. It is for the telephone system. Quoting
- > from FIPS 185: "Data for purposes of this standard includes voice, facsimile

It apparently came close to covering everything. I have heard from several people at NIST describing the general unhappiness there about the EES. One wrote to me:

- > Three weeks ago, Ray Kammer {the deputy director} and Mike Rubin {the
- > general counsel} here told people to rewrite the FIPS 185 (the EES), which
- > was in draft form, so that the standard applied to all electronic
- > communications, including those not covered under the then current language.
- > They refused, even walked out of the meeting, saying that it just could not
- > be done. Ray Kammer backed down, and the FIPS went out w/o the
- > all-inclusive language.

{remarks in curly brackets added by L Hoffman for explanation}

In any case, that point may be somewhat moot because Capstone applies to data!

Re: Denning's thoughts on the Clipper Chip

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Thu, 10 Feb 94 06:11:05 PST

>The standard (FIPS 185) is not a standard for the Internet or any other high >speed computer network. ...

The language sounds to me like it covers ISDN which is rapidly becoming the standard for non-local networking, all switched circuits, which will soon include most cable systems, and standard commercial modems carry the vast majority of all current computer communications. What do you think the superhighway is going to be made of? We have AT+T trying for the twisted pair as the standard, and the cable companies going for a cable version, and some chasing optical, but it is all circuit switched at one point or another.

> ... The standard will make it much

>harder for anyone to conduct illegal taps, including the government.

For someone who lived through Watergate and Irangate and all the other gates, I am amazed that you can still take this position. It only means

that the class of people who will be able to get the information will be restricted to the richer and more powerful. Anyone familiar with the telephone system today knows that to tap a line requires only that the FBI tell the telephone company the phone number. The rest happens in a matter of seconds. With clipper, it will be the same way.

> ... Keys are escrowed so that if someone uses this technology, they cannot > use it against national interests.

How much do these escrow agents get paid, and how well are their families protected? How many guards watch them continuously? Who are we kidding? US Nuclear codes were leaked to the Soviets at the height of the cold war. Do you really think that we will protect these escrow agents any better?

>As near as I know, neither CPSR nor any other group has conducted any >systematic poll ...

I know for a fact that most of the major telecommunications providers are worried that Clipper will be made the standard. The reason is that they need better protection and they have to be able to do more things more flexibly than Clipper allows. They also don't want to have to pay the company who makes clipper a fortune to use a technology they don't want to use.

>Hundreds of people is hardly overwhelming in a population of 250 million ...

Do you claim to believe that the great silent majority is in favor of Clipper? Actually, hundreds of people who opposed it against only a few who supported it would tend to indicate that 245 Million oppose it and 5 million are in favor. Not that this was a statistically valid sample. After all, the people who oppose it are probably more knowledgeable than the general public.

>... concluded it was very strong. ...

In the light of 5,000 years of cryptographic history where experts claimed that systems were very strong only to find them broken soon after, I find it hard to trust the hand picked committee of 5 so-called experts who are given money and time to pass judgement on a technology that is so weak that they are afraid to expose it to the light of day. If it is so strong, why not let the rest of the world review it? The German experts said the same thing about Enigma, and lots of US experts said the same thing about

Clipper Chip Politics

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Thu, 10 Feb 94 09:11:08 -0500

At first I was astounded by the hysteria over the Clipper chip but have come to the conclusion that it is really a matter of Politics and Money - technical worth has nothing to do with it.

Have just finished reading the Cantwell Bill text on export controls and have come to a similar conclusion. Lots of good sounding words modified by vague exclusions. (Could not tell if PGP was permitted since all the user has to do

is install or excluded since each user must generate a unique key).

Clearly, if I were to design a custom mechanism for a client and the client had the only copies in existence, the old rules would apply & if the client were "offshore" I would be in violation.

According to the EFF, Mrs. Denning and I must be the only people publicly on the net who are in favor of Clipper/Capstone as a cheap means for very simple limited protection. It will fill the great void that exists between that which *should* be protected and that which *is* being protected.

In the last few months, virtually every RFP I have seen deals with protection of "Sensitive but Unclassified" information. Presently, this is done with STU-IIIs and DES. Clunky. Ex\$pen\$ive. Requires effort to initiate.

Government agencies faced with field offices, telecommuting, and electronic filing desperately need something that is

- 1) Cheap
- 2) Easy to use
- 3) Blessed by the Government
- 4) Sufficient to deter hackers and reporters
- not because they are personally concerned about disclosure but because public law 93-579 (Privacy Act) and public law 100-235 (Computer Security Act) says they *will*. And for these uses Clipper/Capstone is *good enough* (C).

People bemoan the fact that the government is creating a self-indulgent monopoly, but I have not seen anyone else rushing to fill the gap (three years ago I outlined both in magazines and at conferences a very simple means for access tokens/smart cards such as those from Enigma-Logic, Racal, and Secure-ID to be used to securely encrypt remote dial-up sessions. No one was interested. I have not seen ads for the Beaver BCC-007 encrypted laptop computer lately either.

To me the whole key escrow procedure is a legal sop, I fully expect certain government agencies to be able to break any transmission within seconds given the right equipment and all of the keys (not necessarily who has which, just *all* of them), but I do not really care since anything that needs more protection will just receive stronger encryption before C/C ever sees it. The real value is for authentication and protection from volume analysis. (Today, it is easy to tell which of my missives are protected and which are not. How much and where can be valuable information even without reading the contents. With C/C you will have to decode everything to find out which is important and which is a take-away order).

The NSA/FBI meeting at Bellcore included an assertion that a "National Laboratory" would be required to reverse engineer the chip. Does anyone think that it would not be easier/cheaper to simply buy someone on the inside? "Security by Obscurity" may be effective for short durations and limited value objectives but we are talking strategic value here.

Thus in my opinion, the whole broohah is a smoke-screen. C/C is going to happen, it will do what it is supposed to, it will become a standard since it is going to be cheap and enough, and some organizations are going to make

billions of dollars off it - that is just the American Way.

I still want some to play with. Padgett

Re: Campaign and Petition Against Clipper

Geoff Kuenning <geoff@FICUS.CS.UCLA.EDU> Thu, 10 Feb 94 13:48:28 -0800

In <u>RISKS-15.48</u>, Dorothy Denning combines some good points with some very paternalistic and unsupportable claims. I will primarily address the latter.

>... The Clipper initiative is the result of
>considerable deliberation by many intelligent people who appreciate and
>understand the concerns that have been expressed and who worked hard to
>accommodate the conflicting interests. The decisions that have been made were
>not made lightly.

In other words, despite the fact that many intelligent and well-informed people *oppose* Clipper, "we know best, so stop complaining." The fact that the decision was made by well-intentioned people does not make it correct.

>The standard (FIPS 185) is not a standard for the Internet or any other high >speed computer network. It is for the telephone system.

In the first place, many people access the Internet via various forms of telephone lines. If they are encrypted, it will be easier to tap them if they use Clipper. In the second place, the Administration has been quite up-front about its desire to force key-escrow encryption into nearly every encryption application. So while Ms. Denning is technically correct in her narrow reading of the document, CPSR is equally correct in raising an alarm about the larger issue of high-speed networks.

>As near as I know, neither CPSR nor any other group has conducted any >systematic poll ...

Ah, the old "silent majority" argument. I thought that went out when Nixon resigned.

The truth is that, among the tiny fraction of the public which has expressed an opinion, there *has* been overwhelming public opposition. Very few people have written the Government to say, "my, what a wonderful idea!"

Organizations like TV networks have a multiplier rule they apply to letters, where they figure that every letter received represents N people who felt the same way, but didn't take the time to write. To suggest that only one's opposition took the time to write, and that everyone else is in agreement, is at best disingenuous and at worst intellectually dishonest.

> The ACM is in the process of >conducting a study on encryption. CPSR is a member of the study group, as am

>I. Steve Kent is chair. Our goal is a report that will articulate the

>issues, not a public statement either for or against.

In other words, having attempted to discredit what little data we *do* have, Ms. Denning is stating that there are no plans to conduct a scientific study of public opinion. Perhaps the ACM or the CPSR should fund Roper or Gallup to investigate a few questions, approved by both Ms. Denning and a CPSR representative as being unbiased?

- > The International Association for Cryptologic Research has not to my
- > knowledge made any official statement about Clipper.

I don't see what relevance this has to anything. One organization of cryptologists has remained silent. So what?

- > Hundreds of people is hardly overwhelming in a population of 250 million,
- > especially when most of the letters were the same and came in through the net
- > following a sample letter that was sent out.

The first part of this statement is patently false; the same argument could be applied to any Harris poll. The second part, about "form letter" distortions in public issues, is relevant and important. All the more reason to do a more scientific survey.

- > ... I do not know the facts of the 1970s
- > incident that is referred to here, but it sounds like it occurred before
- > passage of the 1978 Foreign Intelligence Surveillance Act. This act requires
- > intelligence agencies to get a court order in order to intercept
- > communications of American citizens.

The 1978 act was passed in response to the abuses of the early 70's. It should not have been necessary, since the NSA was prohibited from domestic spying even before that, but the NSA figured that since the cables involved were international communications, it was OK to eavesdrop on them. This is a rather classic case illustrating the way the NSA used the loosest possible interpretation of restrictions, rather than actively trying to respect the privacy of law-abiding citizens.

- > I am not aware of any recent evidence
- > that the NSA is engaging in illegal intercepts of Americans.

Once burned, twice cautious. Ms. Denning, think of the egg you'll have on your face if the NSA gets caught misbehaving a few years from now. Personally, I don't see why I should trust any person or agency that is so secretive.

- > The 1987 Computer Security Act states that NIST "shall draw on the technical
- > advice and assistance (including work products) of the National Security
- > Agency."

The question is of who was in control. There is a world of difference between drawing on "advice and assistance," and stepping out of the picture to let someone else do the job. I believe that the latter is what CPSR is worried about.

- > ... I can tell you that it
- > is a fact that new communications technologies, including encryption, have
- > hampered criminal investigations.

Without data or references, how are we to believe this? CPSR carried out, at great difficulty, some preliminary research. There is no indication that they selected that data, and I hope that Ms. Denning is not suggesting this. Again, we have an attempt to invoke the "silent majority" argument to claim that the sampled data is invalid. Only this time Ms. Denning doesn't even offer anything to back up her counterclaim.

In the first place, let's have some facts here. What criminal investigations have been hampered by new technologies? How many?

In the second place, a pervasive thread in Ms. Denning's thinking seems to be that there is no room for a tradeoff between law enforcement and freedom. Let me point out that crime would drop tremendously if the police were allowed to search anyone's home at random, without warning, and to confiscate anything they chose. But I don't think I'd want to live in such a society. Similarly, I'm perfectly willing to let a few criminal investigations be "hampered" or even fail, if it means I can use strong encryption without fear of eavesdropping or prosecution.

> The standard is voluntary -- even for the government.

That's not what I remember. I seem to recall that the original announcement said that the standard would be applicable to all government agencies. Is there a citation to support the claim that it's voluntary within the government?

As to outside the government, yes, it's voluntary. For now. But there are already major pressures being applied to make sure that this "voluntary" standard is the only practical choice. For example, Clipper will be much easier to export than RSA, Idea, or even the venerable Enigma. Government dollars are being used to make sure that the Clipper chip is available and cheap, undercutting the possibility of fair free-market competition. And hints have been dropped that any future encryption made available to the public will also require a key escrow scheme.

Geoff Kuenning geoff@ficus.cs.ucla.edu geoff@ITcorp.com

A huge vote of thanks to all the police, fire, medical, water, power, and gas workers who have worked 12-hour shifts to help us out after the quake.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 51

Thus 10 February 1994

Contents

- FLASH: Vice President Gore Questions Current Key Escrow Policy! Stanton McCandlish
- CMU elections suspended due to computer problems Declan B. McCullagh
- TCAS blamed for near collision over Portland **Lauren Wiener**
- Pacific Bell Customers Get Unpleasant Messages Lin Zucconi
- Two recent UK tales: Gas payment notices; info network problem Peter Ladkin
- FBI falsely obtained wiretap in KC <u>Paul</u>
- Re: "Misunderstanding" a CERT advisory
- Espen Andersen Re: Altered White House Docs

A. Padgett Peterson

Pete Mellor

Jim Hoover

- About Computer Software and Patents **Paul Robinson**
- Info on RISKS (comp.risks)

▼ FLASH: Vice President Gore Questions Current Key Escrow Policy!

Stanton McCandlish <mech@eff.org> 10 Feb 1994 17:55:25 -0600

National Information Infrastructure Advisory Committee met today in Washington at the Old Executive Office Building. In comments made after a question and answer period, Vice President Al Gore said that key escrow policy announced last Friday (4 Feb 1994) had serious flaws and that he hope the issue of who holds the keys and under what terms would be given more serious, careful consideration.

Gore made it clear that some amount of control of cryptography technology was necessary for national security. However, the key escrow policies announced by the Departments of Justice, Commerce & State, and the NSA, were "low level decisions" that got out before thorough analysis. In a conversation with Mitchell Kapor, Esther Dyson, and Mike Nelson (of the White House Staff), Gore said that he would prefer that the keys be held by some part of the Judiciary branch, or perhaps even by trusted, private escrow agents. He made it clear that he believed that the escrow agents named in last Friday's announcement (National Institute of Standards & Technology and the Treasure Department) were no appropriate key holders. Mike Nelson also indicated that there was real interest in a software-based escrow system instead of the hardware-based SKIPJACK standard

Those of us who heard Gore were quite surprised. His remarks suggest that the key escrow policies to date do not have full support of the White House.

Still, Gore was quite firm in asserting that some control of encryption technology is essential to national security. "Encryption and codebreaking have determined the outcome of world wars. He stated (incorrectly) that most our industrialized allies place must stricter controls in encryption that the US does. In fact, almost all COCOM countries allow the export of DES-based products, though some do not allow DES to be imported.

The whole question of encryption was raised when Mitchell Kapor told the Vice President that over half of the Advisory Council members had serious reservations about the current Clipper/Skipjack policies. Gore and Kapor agreed that the Advisory Council should be used to have a serious dialogue about encryption policy. Given Gore's departure from the current Clipper proposals, there might actually be something to talk about.

========

NOTE: This DOES NOT mean that Clipper is going away. Part of stopping Clipper is to lift export controls on encryption and enable US companies to start producing products that enable all of us to protect our privacy with strong encryption.

I urge you to write to Rep. Cantwell today at cantwell@eff.org. In the Subject header of your message, type "I support HR 3627." In the body of your message, express your reasons for supporting the bill. EFF will deliver printouts of all letters to Rep. Cantwell. With a strong showing of support from the Net community, Rep. Cantwell can tell her colleagues on Capitol Hill that encryption is not only an industry concern, but also a grassroots issue.

Again: remember to put "I support HR 3627" in your Subject header.

[For more info on the Cantwell bill, see Stanton's contribution in RISKS-15.47. I have deleted a lengthy repetition here. There is as yet no response from Stanton on Jon Leech's question in RISKS-15.50 on the address cantwell@eff.org. It is presumably NOT Cantwell's. PGN]

Daniel J. Weitzner, Senior Staff Counsel <djw@eff.org> 202-347-5400 (v) Stanton McCandlish <mech@eff.org> Electronic Frontier Foundation 1001 G St, NW Suite 950 East Washington, DC 20001 202-393-5509 (f)

CMU elections suspended due to computer problems

"Declan B. McCullagh" <declan+@CMU.EDU> Wed, 9 Feb 1994 23:33:03 -0500 (EST)

Carnegie Mellon University is known around the world as a technological innovator. To a great extent, this also makes our entire university dependent on technology to function efficiently.

Our reliance on computers and computer networks was made clear earlier today when the results of the student government elections -- for the first time in the history of the school -- could not be validated because a computer system with the master list of eligible students was offline.

As might be expected, the ill-timed computer failure upset quite a few people who wanted to know the results, for this election marked the culmination of a drawn-out dispute between graduate and undergraduate students, who had planned to settle their difficulties at the ballot box.

But the results can't be completely counted until the SIS (Student Information System) verifies that all the candidates -- and suspect voters -- have paid their bills this semester. We're hoping that it's going to be back up tomorrow...

Declan McCullagh Student Govt Treasurer (fortunately, not up for re-election)

TCAS blamed for near collision over Portland

Lauren Wiener < lauren@reed.edu> Wed. 09 Feb 94 21:11:19 -0800

>From the Oregonian , Sat. Feb. 5, 1994, p. B1, B3:

Near collision at PDX prompts investigation

Two commercial airplanes carrying 113 people nearly collided in flight near Portland Thursday afternoon, prompting an FAA investigation into whether an on-board warning system put the planes on a collision course. The pilot of Alaska Airlines flight 548 saw the Horizon Airlines Dash-8 out his window and later estimated it flew within three-fourths to one mile of his plane.

[...deleted paragraph about standard minimum separation of 3 miles...]

The Alaska MD-80 carried 80 passengers and five crew members; the Horizon Dash-8 had 25 passengers and 3 crew. The incident happened at 2:38 PM Thursday and involved the Alaska flight taking off from Portland International Airport and Horizon Airlines Flight 2215 from Spokane, which was on its descent for landing.

Dick Meyer, a spokesman for the Federal Aviation Administration in Seattle, said the Alaska flight was climbing at a normal rate of speed when each plane's Traffic Collision Avoidance System warned of the possibility of collision. The planes were at between 9,000 and 10,000 feet elevation and 12 to 13 miles northeast of Portland when the collision alert was sounded.

The warning system, also known as TCAS, is a computerized warning system now onboard every commercial flight in the United States. It uses radio signals emitted by each plane to determine whether there are other aircraft that are approaching a plane's course. If there are, TCAS sends out a "resolution advisory" consisting of a visual signal and audible warnings telling the pilot to either climb or descend.

Meyer said the Horizon was at 10,000 feet and preparing to descend. The Alaska flight was climbing to 9,000 feet when the TCAS system on both planes went off. "The Horizon flight that was coming in received a TCAS alert that told it to descend. The Alaska plane was climbing at its normal rate and got a TCAS alert that told it to climb," Meyer said. Meyer said the Horizon pilot began dropping to 9,000 feet and radioed air traffic control. The controller, realizing there was a plane coming up to that altitude, got both pilots on the radio and ordered the Horizon flight "to climb and maintain separation," Meyer added.

The two planes eventually flew within less than a mile of each other at the same elevation. "It was the response to the TCAS alerts that caused them to come closer than they should," Meyer said. Meyer said the Alaska pilot filed a near midair collision report with the FAA. Meyer said the incident was being investigated by the FAA and its TCAS program manager in Washington, D.C.

Ted Blahnik, Horizon's chief pilot, said he didn't think the Thursday incident demonstrated any problems with TCAS.

"This is not a glitch," he said. "This thing operated exactly as designed. [!! My *favorite* line!!] The guy who really went into stress mode was the air traffic controller."

TCAS has been on most commercial planes for the past several years. It's been required on all U.S. flights carrying more than 30 passengers since Dec. 30.

Air traffic controllers have been critical of TCAS, saying it is prone to warn pilots of phantom planes and order them to fly into the paths of nearby aircraft.

The National Air Traffic Controllers Association has complained repeatedly about TCAS warnings in busy air space near airports. Controllers have contended that the devices tend to erode the margin of safety because pilots tend to adhere to the warning system rather than rely on the controller's directions.

The association reported in 1992 that about 63% of the TCAS warnings from May 1991 to July 1992 were invalid. Groups representing airline pilots, however, favor the system. They testified before Congress in 1991 that TCAS was a "giant step forward" in preventing flight collisions.

The FAA in May 1991 ordered that some of the TCAS devices on commercial airlines be removed temporarily because they were reporting false alarms. Technical improvements were made since then, and Meyer said that more improvements would be in place by the end of the year "that would make TCAS readings...more definitive."

TCAS systems will be required on all planes carrying 10 passengers or more by 9 Feb 1995.

Pacific Bell Customers Get Unpleasant Messages

"Lin Zucconi" <lin_zucconi@lccmail.ocf.llnl.gov>
10 Feb 1994 09:03:15 U

Pacific Bell customers get messages on voice mail that they'd rather not hear Valley Times (Livermore Valley area), 10 Feb 1994

Electronic hackers have been intruding in to the Pacific Bell voice mail service. "The hackers have broken into the system, altering message greetings and changing passwords, which can keep legitimate users out of their mailbox." Pacific Bell spokeswoman Sandy Hale said that it is a rare occurrence. Patrice Papalus Director of the San Francisco-based Computer Security Institute said "Telecommunications, computer and switchboard fraud is on the increase...Breaking into voice mail is really common."

The article went on to say that two teenagers who were infuriated because they didn't receive a free computer game poster in a magazine promotion broke into IDG's voice-mail system and distributed obscene messages and greetings to female employees. In some cases, customers couldn't get through.

"The violations are unauthorized use of telephone services and a computer crime," said Joe Cancilla, an Asst. V.P. of external affairs with Pac Bell. Etc.

Lin Zucconi zucconi@llnl.gov

Two recent UK tales: Gas payment notices; info network problem

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 10 Feb 94 21:32:59 GMT (Thu)

The Independent newspaper for Tuesday 11 Jan 94, p6 reports that a "Computer upsets 15,000 gas customers". Apparently, 15,000 paid-up customers in British Gas's south-eastern regional area got notices warning that their payments were not up to date, and asking for payment. They complained, and British Gas is sending out apology letters "at a cost of several thousand pounds". The process is automated and "at no stage before posting is any human check made on whether the machine is mistaken." British Gas said that "faulty programming is to blame". (These two last sentences were adjacent. The journalist, Nicholas Schoon, obviously didn't fall for the "dog ate my homework" tale fed him by BG.)

The Independent newspaper for Thursday 10 Feb 94, p2, reports that "Computer flop cost taxpayers \pounds 59m". The system was to provide an `information network' for the department's Training and Enterprise Councils. The article is a little hazy on details that would enlighten RISKS readers, but mentions a

highly negative report on the system by the Commons Public Accounts Committee. (The Commons is the British lower House of Parliament, i.e. the significant part of the governing body of Britain.) Noone bothered to "test a pilot scheme" to see if things worked. The "info network" cost \pounds 48m, and the department had spent \pounds 11m by Sept 92 on 200 management consultants to help with it, despite planning only \pounds 1.3m for this in 1989. But it's really hard to tell from the article how much of this was a computer system that cost too much and didn't fill expectations, and how much was simply bad management.

Peter Ladkin

FBI falsely obtained wiretap in KC

<paul@kuhub.cc.ukans.edu>
9 Feb 94 06:46:21 CST

Quotes from Chief U.S. Magistrate Judge John T. Maughmer regarding FBI wiretaps in a case against now deceased Kansas City financier Frank Morgan:

"...disturbing pattern of material misstatements, overstatements, and omissions" in the government affidavit seeking court permission to wiretap Frank Morgan's office.

"The conduct of the FBI...rises to such a level of recklessness as to mandate suppression" of the evidence obtained through the wiretap.

The judge's comments were included in the 9 Feb 1994 Kansas City Star.

✓ Re: "Misunderstanding" a CERT advisory

ESPEN ANDERSEN <EANDERSEN@HBS.HBS.HARVARD.EDU>
10 Feb 1994 08:05:36 -0400 (EDT)

>Expect journalistic exaggeration.

I can't resist: In 1982 (I think) a Polish climbing team had a fatal accident in the Troll wall ("Trollveggen") in Norway. In the serious Oslo morning paper the climbers were reported to have fallen 600 meters to their deaths. In the liberal afternoon paper, the fall was 800 meters. In the sensational afternoon paper, the figure was 1200 meters.

"Trollveggen" is approximately 1000 meters high.

Espen Andersen (eandersen@hbs.harvard.edu)

Re: Altered White House Documents (nothing new?)

A. Padgett Peterson A. Padgett @tccslr.dnet.mmc.com>

Thu, 10 Feb 94 16:37:33 -0500

It was my understanding that politicians have a "right of revision" to anything that is placed in the Congressional Record such that if they happen to say something in a speech that is later judged to have been "incorrect", the error can be corrected before it goes into the Record.

As a result, it appears that there need not be any correlation between what is said "for the Record" and what actually appears there. So why should we be surprised if the same executive privilege is extended to Whitehouse.gov?

Padgett

★ Re: Altered White House Documents (Firth, RISKS-15.47)

Pete Mellor <pm@csr.city.ac.uk> Thu, 10 Feb 94 12:21:13 GMT

> The relevant quote came to mind immediately:

>

> "He who controls the past controls the future."

My recollection of the intended quotation (from George Orwell's "1984") is:-

"He who controls the past controls the present.

He who controls the present controls the future."

(I haven't looked it up in the book, so my recollection may be inaccurate, too!) Readers may recall that this was the slogan of the "Ministry of Truth" (which was in charge of lies and propaganda) where the hero, Winston Smith, was employed to doctor public archives according to the latest political line which the Party had decreed was the current infallible and unchangeable version of the "truth".

Winston's work was demanding and creative. He would receive old issues of newspapers, which landed on is desk via a delivery spout, and rewrite any articles or news items which did not conform. Where this was not possible, he had to take an item out altogether, and replace it with a suitably anodyne item which he had to concoct on the spot. He would then pop the "incorrect" version into a chute which led directly to the furnace.

Orwell once remarked that what he feared most was "Ghengis Khan with a telegraph". With Stalin, he got more-or-less that. Even Orwell's imagination could not foresee the possibilities for manipulating the "truth" which the advent of the computer has opened up, and the capabilities of electronic communication.

Orwell was also concerned about the decay of language. The Party was in favour of "Newspeak", a language in which it was impossible to express a politically incorrect thought. At its best, this would become "duck-speak", the articulation of sounds in the throat without the involvement of the higher centres of the brain. (Remind you of any political speeches you've heard recently?:-) However, that is a separate concern.

"Orwell, thou shouldst be living at this hour!"

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq, London EC1V OHB Tel: +44 (71) 477-8422, p.mellor@csr.city.ac.uk

★ Re: Controlling the future (Altered White House documents)

Jim Hoover <hoover@cs.ualberta.ca> Thu, 10 Feb 1994 17:15:54 -0700

The quote by firth@SEI.CMU.EDU reminds me of a Polish saying from the Communist era:

"Only the future is certain, the past is always changing."

Prof. Jim Hoover, Dept. of Computing Science, University of Alberta Edmonton, Alberta, Canada T6G 2H1 hoover@cs.ualberta.ca +1 403 492 5401 or 5290

About Computer Software and Patents

Paul Robinson <PAUL@TDR.COM> Thu, 10 Feb 1994 00:59:30 -0500 (EST)

The following represents the text I will be reading at the Patent Office hearing on the relationship between computer software and patent issues, Crystal City, Virginia, 9:15am February 10. This text has been edited to allow me to fit it, and possible questions, into an 11 minute space.

This is a short portion of my remarks on the matter. This will be part of a complete comment on the Federal Register text. My comment will be posted to the Internet once completed.

Good Morning Commissioner Lehman, Mr. Kushan, the staff here, members of the audience, people reading this report in the future and anyone else I've forgotten.

My name is Paul Robinson. I am Chief Programmer for Tansin A. Darcos & Company, a software development firm specializing in text processing applications; I also do work on Commercial Philosophy and metaphysics of computer systems. My special interest and my personal hobby is collecting compiler and other program sources. My reasons for this are that these all solve problems. By reading the manner and method other people have solved other problems, it gives me insight into how to solve mine.

This is a common practice in the computer world in order to, as the expression goes, "Not reinvent the wheel." I assume this is common in other industries. In fact, this is most likely the reason that we have a patent system; someone is granted the exclusive right over commercial use of an invention for a

limited term in exchange for telling the world about it.

For most computers, every application such as word processing or spreadsheets has at least two and possibly three or more different applications fighting for market share. The fights in this industry are usually referred to by the expression "Dinosaur mating dances" as huge companies fight for market share by releasing new programs to introduce new features that the companies believe the customers want. Version 3 of Turbo Pascal was an excellent language compiler and less than 40K. Version 4 would fit on one 360K diskette. Today, Turbo Pascal for Windows version 1.5 takes 14,000K of disk space. The program that is probably the premiere application for graphics design is Corel Draw!, which has so much material it is now being released on not one, but two 500 megabyte CD-Rom disks.

But there are probably still niches for smaller companies to move into.

With the rapid changes in the marketplace, it is necessary to be ready to have new programs and new releases of old programs out to encourage people to move to the next release. In some cases, companies make more money from upgrades, and need to do so to stay alive. These kind of cycles mean new releases have to be out very quickly; in a matter of weeks to months.

With this kind of rapid development cycle, delays in the release of a program could be fatal and the time available to create the work is sometimes barely enough. Until recently, the only legal issue that anyone had to worry about was copyright infringement. That could be avoided by creating new work from scratch.

Now we have another issue altogether. A programmer can independently create something without ever knowing about any other developments, and yet be sabotaged by the discovery that the method that they used is patented. This is a standard problem that all industries have had to face, and it is part and parcel of living in an industrial society. But there is another problem. A computer program is the written instructions by a human being to tell a computer how to perform a particular task. As such, there are only two parameters: the input supplied to the program and the expected output. Everything else is literally a figment of someone's imagination.

This bears clarification. A computer program is the means of manipulating the internal data paths of a computer system. There is no requirement that the manipulations have any correspondence to the real world. In this, the real world, doing anything requires the expensive movement of people and goods from one point to another, the possible refinement of materials into other materials, and the expenditure of energy and resources. Doing anything in a computer is merely the essentially cost-free movement of electron paths from one direction to another; it brings forth the apportation of the concepts of the madman Imanuel Kant into reality: a world in which anything is possible:

- We can see this in the current discussions going on about violent computer games where someone goes about maiming, shredding and killing their opponents, in graphic detail, then when the game is over, nothing in the real world has changed except the clock. One of my favorites happens to be the game "DOOM" where the weapon of choice is a 12-gauge shotgun, but a chainsaw does a nice job on people close to you.

- We have seen it in motion pictures such as "Total Recall", where, if one is acting within a part of a computer program, you cannot be certain what is real or what is fantasy. The movie "Brainstorm" had simulations of sexual contact apparently indistinguishable from reality.

There are things that can be done within a computer program that cannot be done in the real world, or would have undesirable consequences. As such, we should ask whether the patent rules, which are designed to apply to real-world conditions where doing something requires the expenditure of energy and resources, should apply in a world where the known rules of the universe do not apply. Because the entire design starts from scratch, and the designer doesn't just get to play God, he <italic>italic> God.

Despite the ease under which someone can do something, we still live under real-world constraints. Once a design choice is made, it is very expensive in time and effort to change it. Worse, because most programs have interactions that cover every part, a change to one part can cause unexpected and even undesirable side effects in unknown and unexpected places. Computer programs may be "the stuff that dreams are made of" but once placed into concrete form as written in software instructions, it's just as expensive to repair or change as if it was carved out of real materials.

It may be necessary to change the rules on patents to comply with the conditions that exist for computer programs.

There has been talk of instituting "first to file" in order to "harmonize" with the systems in other countries; I think that is not a good choice; most countries have fewer patents, and provide protection which is much narrower than our system does. This would also mean that someone who does invent a new and useful technique for use in a computer application would be unable to collect any royalties from someone else who is using the same invention, who thought of it after they did, but started using it before they filed.

The two really large problems that exist in our system are probably two part: the secrecy under which patent applications are filed, and the problems if a program uses parts of several patents, which might not be discovered until later.

As I mentioned earlier, computer programs are created out of the figment of someone's imagination, then mass copied, the way an original painting can be reproduced by lithograph. A single large application might have a dozen people working on it, and upwards of 50 different features, and might have upwards of 200 or more different parts, any one of those might be infringing on zero, one or more patents depending on what the claims are. I doubt seriously that all but the largest corporations have the resources to do 200 patent searches on a single software application, which would be prohibitive for a small company, because it is likely that a large program could infringe dozens of patents, due to the continued development of ever larger applications that do multiple simultaneous functions.

But more than that, you can't do patent searches on works which are under application form, until after the patent has been issued. And more

importantly, with more than 1,200 patents issued every week, checking them all for possible interconnection would make it impossible to do any serious work.

Seventy years ago, fears that the major piano player manufacturer would tie up the entire song market and prevent other companies from creating player piano rolls caused Congress to institute compulsory licensing. This may be an idea whose time has come again.

Therefore it might be considered to make two changes in the patent law with respect to computer programs: to implement a standard compulsory license, perhaps 10 percent of the manufacturer's suggested list price, and to eliminate secrecy provisions in the filing of patent applications.

Either of these could certainly help the situation. Eliminating secrecy and publishing applications once filed would let people know about pending inventions: they could endeavor to avoid infringements in advance; it might also allow them to file interferences early, if it turns out that they invented the concept earlier, while it is cheap to do so; and would allow people to be aware of what is being developed which would comply with Article 1, Section 8 of the Constitution, where patent protection was designed "to encourage the improvement of the useful arts".

The other option of setting a standard royalty via compulsory license would eliminate the worries of someone infringing upon an existing patent or one that is filed after their work is created. It would also grant to inventors an income stream from those who use their inventions, which started before they filed their application but after they reduced the invention to practice. It would also limit liability and exposure to sustainable limits. As it stands, if someone develops a program that infringes upon 40 patents, and they each want a 3% royalty, it isn't hard to see that 120% of the program's income is not going to be possible.

Paul Robinson - Paul@TDR.COM



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 52

Friday 11 February 1994

Contents

- Cygnus Support frees its security software to beat Internet break-ins John Gilmore
- Re: Campaign and Petition Against Clipper

Dorothy Denning

Marcus J. Ranum

Carl Ellison

Paul R. Coen

- Re: Notes on key escrow meeting with NSA
 - Roy M. Silvernail
- Re: Coincidences (Sniffers, Breakins, and EES)

A. Padgett Peterson

- Re: Verify your backups
 - Li Gong
- Re: Electronic Keys vs. The Old Kind

Morgan Price

- * New List on Computer/Telephone Problems/Bugs/Viruses/Dangers
 - Paul Robinson
- Info on RISKS (comp.risks)

Cygnus Support frees its security software to beat Internet break-ins

John Gilmore <gnu@cygnus.com> Thu, 10 Feb 1994 09:49:52 -0800

> Cygnus Support Frees Its Security Software To Beat Internet Break-Ins

MOUNTAIN VIEW, Calif., February 10, 1994 - Cygnus Support today announced public availability of its Cygnus Network Security (CNS), a software solution to guard against the recently publicized rash of break-ins over the Internet. Cygnus Network Security is a freely available, stable, tested version of Kerberos, the well known network security software.

Cygnus Support is giving CNS to the public in an effort to protect users of

the "data superhighway". The Internet community gains an immediate solution for this break-in problem. Organizations can then contract with Cygnus to develop more comprehensive long-term security strategies.

The rapid evolution of information technology has opened the doors of communication while leaving many sites vulnerable to break-ins. The Computer Emergency Response Team (CERT) reported last week that intruders had captured access information for tens of thousands of systems across the Internet. CERT advised all Internet users to change passwords, but this is not enough to prevent this type of break-in in the future.

"This security vulnerability has been there for a long time, but the crackers have only taken advantage of it in the past year," said Michael Tiemann, president of Cygnus Support. "It's well past time to solid countermeasures. Kerberos is the only protection that's freely redistributable, software-only, well supported and ready for use today."

CNS prevents passwords from being sent over the Internet in clear text. Kerberos uses DES encryption to validate the user's password on a local machine, rather than sending it across the net to a remote machine. This prevents the password from being captured off the network and used by crackers. CNS provides network-level security and eliminates the single largest risk that Internet users face today.

Cygnus Network Security software is offered free of charge over the Internet, and is available by calling Cygnus Support at 1 800 CYGNUS-1 or +1 415 903 1400. Due to U.S. export policy, Kerberos is only available in the United States and Canada at this time. After calling Cygnus Support and verifying their location, users will be told where on the Internet to download the software. CNS includes installation notes, complete source and binary code, and preliminary documentation. The Internet release is provided as-is and without support; users who want help with installation or use must contract with Cygnus for it. CNS binaries are provided for these Unix platforms: SPARC (both OS's), DECstation, HP 700, and Sun-3. CNS is not currently available for PC's or Macintosh. Other platforms are under development.

Commercial support for Cygnus Network Security is available from Cygnus Support. Cygnus offers installation support, fast maintenance response, printed documentation, periodic releases, and custom development work, including ports of CNS to specific platforms. Customers need not be on the Internet to use Cygnus Network Security support. Prices start at \$5000 and vary depending on the number of users supported.

Cygnus Support was founded in 1989 to provide commercial support for sourceware. Sourceware is supported, centrally managed software whose source code is openly available. Cygnus provides a full range of products and services for software developers, including site support, custom development, and open systems solutions, in North American, Europe, and Asia. The company is based in Mountain View, Calif., with an office in Cambridge, Mass.

To get copies of the software, call +1~800 CYGNUS 1 or +1~415~903~1400, and say you want the free Kerberos software.

Press contacts:

Erin McCormick Terri Thatcher, <terri@cygnus.com>

Cunningham Communication Cygnus Support

★ Re: Campaign and Petition Against Clipper (RISKS-15.48 and 15.50)

Dorothy Denning <denning@cs.cosc.georgetown.edu> Fri, 11 Feb 1994 14:09:16 -0500 (EST)

The following comments are in response to responses posted in <u>RISKS-15.50</u> on my earlier comments in <u>RISKS-15.48</u>:

>From Marc Rotenberg:

>

- > The NSA is responsible for foreign signal interception. It has no legal
- > authority to conduct wire surveillance. What are the NSA's "national
- > security" interests in domestic wire surveillance?

I do not believe that NSA has any particular interest in domestic wire surveillance. I expect their concern is that if a product with a very strong algorithm such as SKIPJACK were to be manufactured without keys being escrowed, then such products would be very attractive on the foreign black market (presumably, such products would not be exportable) where they could interfere with foreign intelligence.

- > The FBI made certain claims that cryptography was impeding criminal
- > investigation conducted by wiretap. CPSR investigated the FBI's claims by
- > filing a Freedom of Information Act suit to obtain the relevant documents.
- > The documents provided to us by the Department of Justice revealed that none
- > of the FBI field officers had encountered any obstacles. The Department of
- > Justice has just informed us that they provided to us all relevant documents
- > concerning the Clipper proposal.

In testimony before the Computer Systems Security and Privacy Advisory Board (CSSPAB) at NIST, James Kallstrom of the FBI said that encryption was stymying the effort in more than three but less than ten of ongoing cases. The FBI does not give details of ongoing investigations, so this information would not be available through FOIA.

- > There is one reported case where cryptography made it difficult for law
- > enforcement to obtain evidence. That case concerned reading the contents of a
- > file on a hard disk after it was seized.

>

- > If this is the problem that the Clipper proposal is intended to solve, then
- > the key escrow scheme must be extended to every single encrypted file -- not
- > just encrypted communications -- everywhere in the world.

I've heard of 3 cases now where encrypted files could not be decrypted, but law enforcers seem to be much more concerned about communications than stored files. Clipper does not address file encryption.

> An FBI legislative proposal now under consideration at the White House would > mandate a Clipper-like scheme. That proposal is backed by fines up to \$10,000 > per day and jail time.

Everything I've seen has said Clipper is voluntary. Quoting from the standard: "This standard does not mandate the use of escrowed encryption devices by Federal government agencies, the private sector or other levels of government." Dept. of Commerce, NIST, Docket No. 930659-4017, RIN 063-AB19, Approval of FIPS 185, Escrowed Encryption Standard (EES).

- >> I support this objective. Unfortunately, it is not
- >> possible for most of us to be fully informed of the
- >> national security implications of uncontrolled
- >> encryption. For very legitimate reasons, these cannot
- >> be fully discussed and debated in a public forum.

>

- > This assertion has never been supported by evidence. It has been used simply
- > to stifle criticism.

Certain information relating to foreign intelligence operations is classified. Are you saying that decisions should not be based on classified information or that foreign intelligence information should not be classified?

- > CPSR did not participate in the inter-agency policy review. Our position from
- > the very beginning is that these decisions must be made openly.

As part of the inter-agency review, the CSSPAB was asked to sponsor hearings on the proposal. These were held in June. The testimony that was presented was given to the government. Marc gave a presentation at those hearings, as did David Banisar of CPSR. Several people in the government who have been participating in the inter-agency review were present at the hearings. There have been several other forums as well, including one sponsored by CPSR last June. Again, several people participating in the inter-agency review were present.

- >> In the absence of understanding
- >> the national security issues, I believe we need to
- >> exercise some caution in believing that we can
- >> understand the full implications of encryption on society.

>

- > This premise, if accepted, would mean that people in the United States would
- > have no right to express political views when the government claimed "national
- > security." Certainly, there are matters of national security that must be

I did not mean to suggest that people should not express their views. Being cautious is different from being silent.

>From George Talbot:

>

- > Second, law enforcement needs to get a court order to intercept phone
- > communications. I know of no such need to get a court order to intercept
- > communications on a high speed network w.r.t. Capstone. The current
- > administration proposal does not require a court order to get the escrowed

> keys themselves.

You need a court order to intercept any electronic communications, including those on high speed nets. You need a court order to get keys. Although the court order is not given to the escrow agents (to protect the identity of those under investigation), certification that one was obtained must be presented to the escrow agents. In addition, this certification must be confirmed by an attorney associated with the U.S. Attorney's office (for a Title III federal wiretap) or an attorney associated with the DOJ Office of Intelligence Policy and Review (for a FISA wiretap). For a local wiretap, the certification must be submitted by the principal prosecuting attorney of the state or political subdivision thereof.

Fred Cohen wrote:

>

>>Hundreds of people is hardly overwhelming in a population of 250 million ...

>

> Do you claim to believe that the great silent majority is in favor of Clipper?

No I do not. I was merely attempting to point out what I believed was RISKy logic.

>

- > In the light of 5,000 years of cryptographic history where experts claimed
- > that systems were very strong only to find them broken soon after, I find it
- > hard to trust the hand picked committee of 5 so-called experts who are given
- > money and time to pass judgement on a technology that is so weak that they are
- > afraid to expose it to the light of day. If it is so strong, why not let the
- > rest of the world review it? The German experts said the same thing about

We were not paid. The main reason for not making the algorithm public is that one could build inter-operable products that bypassed key escrow, but that took advantage of the very strong algorithm.

>

- > Why is it that you think you understand more about the implications of
- > cryptography on national security than the rest of us? This elitist crap has
- > got to end. It is bad for our country to have elitists who believe they know
- > more than the rest of us dictating how we will live our lives. It is bad for
- > our country that the esteemed members of this forum do not have access to your
- > rational in order to openly discuss your points of view. It is bad for our
- > country that professors at universities tell their students and the public not
- > to think about the issues, but to trust that the professors know best. If you
- > want to serve the national interest, get the debate out in the open!

>

I did not mean to suggest that I understood the national security issues. I do not. Nor did I mean to suggest that people should not think or talk about the issues.

Dorothy Denning

★ Re: Campaign and Petition Against Clipper (Kuenning, RISKS-15.50)

Marcus J. Ranum <mjr@tis.com>

11 Feb 1994 14:52:03 GMT

Geoff Kuenning writes, with respect to NSA: >Personally, I don't see why I should trust any person or agency that is so >secretive.

This is the same logic that many fear would be applied by law enforcement against people using non-approved non-clipper crypto: "if they aren't using clipper, they must have something to hide."

Funny how the better swords tend to be double-edged. mjr.

★ Re: Denning's Clipper defense (RISKS-15.48)

Carl Ellison <cme@sw.stratus.com> Thu, 10 Feb 1994 19:33:44 -0500

Prof. Denning has issued a defense of the Clipper proposal (which she advocated in a CACM article long before the initiative was announced). Her specifics are easy enough to refute and I'm sure others will do so. However, she closes with an idea so radical that it shocked me.

Her idea that we citizens need a security clearance in order to enter the debate over whether or not we should give up a right we've had for all time (to make, use, disseminate, ..., our own strong cryptography, interfering with the government's ability to spy on us) is so radically off base that the technical debate pales by comparison.

My grade-school social studies teacher is doubtless spinning in her grave. On this point, I would like to hear from newly freed members of the Eastern block.

- Carl Ellison

Re: Campaign and Petition Against Clipper

"Paul R. Coen" <PCOEN@DRUNIVAC.DREW.EDU> Thu, 10 Feb 1994 11:43:03 -0500 (EST)

This is a reply to Dorothy Denning's message in Risks 15.48:

>... A telephone system

>for purposes of this standard is limited to a system which is circuit switched >and operating at data rates of standard commercial modems over analog voice >circuits or which uses basic-rate ISDN or a similar grade wireless service."

The wire running to your house will be part of the basic telephone system, just as it is now. And with "standard commercial modems" becoming much faster in the next year or so, I expect them to last longer. As far as the "analog" part goes, they're trying to take care of that, too.

>The standard will not make it any easier to tap phones, let alone >computer networks.

No, but the Digital Telephony requirements will -- more on that later.

>Law enforcers still need to get a court order just to intercept the >communications in the first place,

Law enforcement does. Those with national security concerns have a much less stringent procedure, if I'm not mistaken. I think it's a bit more than throwning a brick in the air and chanting "National Security" three times, but not much. And if someone overseas is dumb enough to use Clipper, it's pretty easy as well.

>The standard will make it much harder for anyone to conduct illegal taps, >including the government.

I'll buy that up through the "including the government" part. You can't prove that the escrow system cannot be compromised. And the DOJ stated that if the procedures are not followed, it will not be grounds to throw out the evidence.

>Keys are escrowed so that if someone uses this technology, they cannot use it >against national interests.

So it's for our own good?

>As near as I know, neither CPSR nor any other group has conducted any >systematic poll of industry, professional societies, or the public. While >many people have voiced opposition, there are many more organizations and >people who have been silent on this issue.

I thought the NCSA did a survey of IS professionals, and found that they opposed Clipper by 260 to one. I don't know how systematic or not that survey was, however. Perhaps you or someone else has more information.

>The 1987 Computer Security Act states that NIST "shall draw on the technical >advice and assistance (including work products) of the National Security >Agency."

Advice is one thing. However, it does seem that the NSA is capable of either officially or unofficially scrapping any crypto scheme it doesn't like -- for any reason.

>The standard is voluntary -- even for the government.

Do you think that will last? I can't see how it is going to avoid becoming either a requirement or a de facto requirement. It's really doomed otherwise. Or are they going to make it a crime to encrypt communications for the purpose of criminal activity with something other than Clipper?

>For very legitimate reasons, these cannot be fully discussed and debated in >a public forum.

Convenient, isn't it?

>Unfortunately, it is not possible for most of us to be fully informed of the >national security implications of uncontrolled encryption.

We already have uncontrolled encryption outside of the United States. Folks in other countries are just as clever as we are, and there are a lot of articles about encryption in general out there. So what are we doing here? In order to insure that some folks don't misuse the technology, there's a built-in feature for decoding the communications. The FBI knows full well that only "dumb criminals" are going to use Clipper. So what does that mean? In order to protect us, the government wants us to use an encryption technology that they can unlock -- a technology that none of the "real threats" are using?

>It is even difficult to talk about the full implications of encryption on >law enforcement.

Why? I think many of us have a pretty good grasp of the issue. And I think that if you look at the number of wiretaps and the number of cases where encryption technology was a problem, you'll find that few really made a difference in a case. Wiretaps are not that useful in many ways. Informants, financial records, physical evidence, and "bugs," either planted on people or in locations are far more useful.

>The Feb. 4 decision was made following an inter-agency policy review, >headed by the National Security Council

And we all know the extensive confirmation process that appointees to the NSC goes through in the Senate, thus giving the legislative branch a measure of oversight. Oh, wait, that must be in some other reality. Sorry. This is the reality where more and more tasks have been shunted over to "groups" and "councils" outside of the normal channels of oversight.

>considerable input from industry, CPSR, EFF, and individuals as well as from >law enforcement and intelligence agencies.

And surprisingly enough, the government decided to place the government's priorities first.

>In the absence of understanding the national security issues, I believe we >need to exercise some caution in believing that we can understand the full >implications of encryption on society.

"Trust the government." No thank you. Various agencies and departments have done little to earn that trust, and have shown a willingness to violate the Constitution for "greater interests" that turned out to not be so great.

>Interagency Working Group on Encryption and Telecommunications, chaired by the >White House Office of Science and Technology Policy and National Security >Council, with representatives from Commerce, Justice, State, Treasury, FBI, >NSA, OMB, and the National Economic Council.

Ah, yes. The IWGET. Chaired by whom? Oh, I see. No oversight, no accountability.

>The group is to work with industry and public interest groups to develop >new encryption technologies and to review and refine encryption policy.

Oh, and also to resurrect the Digital Telephony issue. You forgot that one. >From the press release:

In addition, the working group will coordinate Administration policies regarding digital telephony. As more and more telephone companies install high-speed, digital communications links, it becomes more and more difficult for law enforcement agencies to conduct wiretaps. The working group will work with industry to ensure that new digital telecommunications systems are designed in a way that ensures that do not prevent court authorized wiretaps.

I'm really having a hard time with Clipper. Depending on which spin you look at, it's either a totally pointless, massive waste of time and money that nobody in their right mind will adopt, or else it's an Orwellian plot to push an encryption technology that Uncle can break. Neither view is really attractive. I'd actually bet more on the first. Or is this whole issue a smokescreen? Is this just an attempt to try to co-opt the issue of liberalization of encryption regulations? Or is it an attempt to make the digital telephony proposal more palatable?

Paul Coen, Drew University Academic Technology | pcoen@drunivac.drew.edu

★ Re: Notes on key escrow meeting with NSA (Blaze, RISKS-15.48)

Roy M. Silvernail <roy@sendai.cybrspc.mn.org> Thu, 10 Feb 1994 22:45:12 CST

- > The LEAF field contains 80 bits for the traffic key, encrypted via the unit
- > key in "~a unique mode <grin>~", 32 bits for the unit id, and a 16 bit
- > checksum of some sort. (We didn't waste our breath asking what the checksum
- > algorithm was.) This is all encrypted under the family key using "~another
- > mode <grin>~".

One of my concerns from the beginning of the Clipper/Capstone proposal was that the LEAF would not be protected to the same extent as the primary traffic. This paragraph confirms that the LEAF is encrypted at least differently.

The RISK here is that the session keys may be vulnerable to a less rigorous cryptographic attack than the traffic itself. So it may not be necessary to even go through the dance with the escrow agencies to compromise a Clipper/Capstone chip. Of course, the Skipjack algorithm would still be required for decrypting the traffic, but it would still appear that this is a vulnerability. I wish this point had come out earlier.

Roy M. Silvernail roy@sendai.cybrspc.mn.org

Coincidences

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Fri, 11 Feb 94 12:03:08 -0500

"Once is happenstance, twice is coincidence, three times is enemy action" _You Only Live Twice_ by Ian Fleming

On February 3rd, the CERT issued a warning concerning password breaking sniffers that had compromised thousands of passwords on the Internet. This was picked up by thousands of newspapers.

One line read "The best long term solution...is to reduce the transmission of reusable passwords in clear-text over the network."

I am told that this problem had been known by experts for quite some time before the alert.

On February 4th, the administration reaffirmed the Clipper/Capstone initiative.

Now I am waiting for the announcement of a "Capstone Ethernet Card" that will protect "Information Superhighway" users from such sniffers. Number three ?

Padgett

Re: Verify your backups

Li Gong <gong@csl.sri.com> Fri, 11 Feb 94 14:03:27 -0800

tsm@cs.brown.edu (Timothy Miller) suggested in RISKS DIGEST 15.49 that lost files (because of failed backups) could be restored from the many mirror sites. Professor Jerome Saltzer of MIT argued in a paper at the SIGOPS European Workshop (1990) that large scale replication may indeed eliminate the need for the kind of backup being done today. See ACM Operating Systems Review 25(1):81-82 for details.

Li Gong, SRI International, Computer Science Lab, Menlo Park, CA 94025, USA

Electronic Keys vs. The Old Kind (Kaiser, RISKS-15.47)

Morgan Price <mprice@BRAHMS.CODA.CS.CMU.EDU> Fri, 11 Feb 94 17:17:17 EST

- > An electronic key with a chip in its tip is to be marketed by the
- > locksmiths, Chubb Security of Sunbury-on-Thames. The key, called
- > Eloctro, has a tiny silicon chip which stores a unique number

> ranging from 10 to 70 000 billion. >Several rather evident risks there.

But compared to the technology it replaces, I think not. There's a lot of trained locksmiths, and a much smaller number of hackers with oscilloscopes.

-- Morgan Price

✓ New List on Computer/Telephone Problems/Bugs/Viruses/Dangers

Paul Robinson <PAUL@TDR.COM> Fri, 11 Feb 1994 13:38:11 -0500 (EST)

This is to announce the creation of a list for the public disclosure of bugs, system problems, viruses, and any other conditions in a computer system that people should be aware of so they can fix the problem.

It is also appropriate to report security holes, dangerous conditions in PBXs, cellular and wire telephone systems, and other computer-controlled devices. Also reports of things such as default accounts and passwords on systems that should be changed, etc.

The focus will be on reporting clear descriptions of problems including how to generate them. The idea being that this will alert people to the nature of certain problems that they might be unaware of. Reproducing these conditions lets others know what is being done, and can allow people to post solutions on how to block them.

The purpose in creating this list is that currently, the only means currently available for reporting discovered security holes in computer systems and possibly other areas is via the Computer Emergency Research Team (CERT) out of Carnegie Mellon University.

The problem with CERT reporting is that the reports generally tend to be done in secrecy, and it fails to let system administrators and others know about what is happening so that these things can be fixed. In short, CERT acts like a black hole and takes too long to publicize problems until lots of places get hit because they didn't know about it.

Some people feel that reports should not be publicized because potential reports might become available to "the bad guys." Well, the truth of the matter is that "the bad guys" trade their discoveries around all the time; the current use of secrecy is only hurting "the good guys" who want to protect their systems.

This list has just been created, and pending creation of an automated processor will be temporarily moderated since my current equipment does not yet tell me what address the message is sent to. This will be changed in the next two weeks.

There will, however, be two addresses. The general list will be

PROBLEMS@TDR.COM

which is used to post a report to the list. To subscribe to the list, use

PROBLEMS-REQUEST@TDR.COM

Currently, both addresses are moderated. This will change shortly as I upgrade the software on my system. Persons wishing to make a report but not be identified should state so in the text of their message. In the future, they will do so by using the -request address which will come to me directly.

Persons wanting to receive this service by facsimile should contact me for details. All messages requesting subscriptions or posting information will be acknowledged. Please pass this announcement around.

It is my intent to set this up such that people can publicly report known bugs, viruses and problems in clear detail so everyone knows about them and can encourage much faster response to these problems than is currently available. It may even embarrass some manufacturers into making fixes sooner when their errors are glaringly exposed in public.

Paul Robinson - Paul@TDR.COM

[I presume that RISKS will try to avoid duplication of detailed discussions with PROBLEMS, but may provide summary information and pointers to issues, as appropriate. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 53

Satagee 12 February 1994

Contents

Electronic tax filing: MAKE.MONEY.FAST ???

Ed Ravin

Celebrity Risks -- Bill Gates

Jack B. Rochester

Computers and Health

Computer User Family

Microsoft Software Development Network registration

James Briggs

Re: FireFly in the Ointment

Andy Kostic

Marco Barbarisi

Re: Sounding the Alarm

Anthony E. Siegman

Georg Feil

Re: Don't trust the phone company

Joe Konstan

Spencer W. Thomas

Michal.Jankowski

Nancy Griffeth and others

Info on RISKS (comp.risks)

✓ Electronic tax filing: MAKE.MONEY.FAST ???

Ed Ravin <eravin@panix.com> Fri, 11 Feb 1994 20:14:53 -0500

An AP article in NY Newsday on 11 Feb 1994 describes a Congressional hearing where prison inmates told lawmakers how they used electronic filing of tax returns to defraud the Internal Revenue Service.

Here are some salient highlights:

* "I think the IRS is detecting maybe 25 percent of the fraud taking place with electronic filing..." -- Frazier B. Todd Jr., serving 2 1/2 years for

collecting more than US \$500,000 over two years by issuing false W-2 forms from fictitious companies in the names of people too poor to file income tax returns. Todd was able to obtain permission from the IRS to file electronically via mail. His frauds continued after he was caught, by processing phony returns through legitimate tax preparation firms. Registering the false companies with the IRS took only a phone call...

- * A convicted tax preparer (doing 18 months) testified how he obtained US \$750,000 over three years in undeserved refunds on behalf of his clients, by inflating deductions and other devices...
- * IRS Commissioner Margaret Milner Richardson says the agency has put new computer "filters" in place to spot fraudulent returns. They've already detected 200 schemes involving 3000 or so false claims (and the tax season is only six weeks old).
- * During the first 10 months of last year, the IRS detected 61,000 fraudulent returns totaling US \$110 million -- but a consultant's report says the true cost could be more like billions of dollars.
- * Representative JJ Pickle (D-Texas) threatens to recommend a freeze on electronic filing if the problems can't be worked out. Commissioner Richardson claims that "electronic filing is the very thing that has allowed us to detect fraud".
- * The speed at which refunds are issued to electronic filers makes it difficult for the IRS to stop questionable refunds. A General Accounting Office staffer suggests that "The IRS has often appeared more interested in expanding electronic filing than in ensuring that it was fully understood and adequately addressed the associated risks"...

[This is sounding all too much like William Gibson's novel _Neuromancer_, where rogue computer jockeys could reap money out of the cyberspatial ether by crashing into big computers and tampering with data...]

Ed Ravin eravin@panix.com +1 914 448 4737

Celebrity Risks -- Bill Gates

"Jack B. Rochester" <0002757498@mcimail.com> Thu, 10 Feb 94 13:30 EST

The Jan. 10, 1994 issue of The New Yorker has a long, juicy article entitled "E-Mail From Bill," detailing a month-long electronic correspondence between Bill Gates of Microsoft and the reporter, John Seabrook. Seabrook is apparently somewhat new to computers and e-mail (someone says to him, "Well, hey, you're not a digital guy!") and his innocence provides a refreshing look at our industry and its leading personality -- you would NOT see such an interesting, forthright, or provocative piece on Gates in, say, PC Computing.

While the risks (as I see them) are not lethal, they are interesting and worth noting:

- 1. E-mail will not replace old-fashioned letter-writing as a form of personal expression. It's essentially an informal business medium for communicating facts, not for sharing Deep Feelings. Even so, in the Gates-Seabrook exchange, it soon escalates/degenerates (depending on your point of view) into ego-aggrandizement and, ultimately, an unintentional psychological profile of Gates, provided by he himself (sans any Smileys). At one point Seabrook asks "How does the rapid change in the power of microprocessors make you feel?" Gates replies, "Feelings are pretty personal."
- 2. Good grammar and proper punctuation are not required in e-mail, and their absence does not seem to affect regard for that person. Seabrook notes the absence of a salutation, complimentary close, or any letter-style boilerplate (e.g., "nice to hear from you", "best regards", etc). Gates often confuses or misuses _its_ and _it's_, something that would be looked askance at in a business letter, but not on e-mail. (However, just to be on the safe side, maybe Gates ought to be using Word for Windows 6.0, with all that fancy on-the-fly correction capability, to draft his e-mail.)
- 3. Finally, the risks of notoriety. Gates talks about his forthcoming marriage ("Being married I don't think is that big a change."), and when asked about wealth corrupting, replies "Absolutely. Hey. Being in the spotlight is a corrupting thing. Being successful is a corrupting thing. These are very dangerous things, to be guarded against carefully. And I think that's very, very hard to do."

In the final e-mail exchange with Seabrook, Gates is asked what he thought of Henry Ford:

Ford is not that admirable -- he did great things but he was very narrow minded and was willing to use brute force power too much. His relationship with his family is tragic. His model of the world was plain wrong in a lot of ways. He decided he knew everything he need to fairly early in his life.

Computers and Health

<cuf@aol.com> Thu, 10 Feb 94 22:22:38 EST

The Computer User Family (CUF) is concerned about the health problem associated with computers. Video Display Terminals, emit UV and ELF radiation and may cause cancer, immune system irregularities, miscarriages and eye fatigue. Computer noise from fans, disk and CD drives is also becoming a source of anxiety, stress and general discomfort. We usually don't realize how loud our computers are: 50dB and more. These problems should be dealt with and add-ons should be provided for present computers to avoid putting us at risks. Some safe screens and quiet power supplies are coming out but they are marginal and prices are prohibitive.

Meanwhile the general guidelines for the users are:

1. Position yourself approximately 22 inches to 28 inches (arm's length) from

the screen and four feet from the sides and rear of other terminals.

- Eliminate sources of glare and lower light levels in the room. Don't sit facing a bright window. If necessary, use screen hoods, glare shields over the screen or wear anti-UV/anti-glare glasses.
- Put a noise absorbing mat under your computer. Pull your computer away from the wall or any hard surface that reflects noise and vibration back to you.
- 4. Rest occasionally during periods of intense concentration. Closing your eyes helps.
- 5. Turn off the VDT when not in use.

✓ Microsoft Software Development Network registration

James Briggs <jeb@vigard.mef.org> Thu, 10 Feb 1994 15:56:00 -0500

The Microsoft Software Development Network (MSDN) programme has lost my registration twice in Canada and 3 times in the United States (the US number is 1 800 759 5474). This has caused about 10 months of frustration. Registering means you give a credit card number and an address. In return, you are sent a CD-ROM every quarter.

Today I tried to change my address for future mailings. The operator took my name, then told me that there was no record of my registration. It appeared lost yet again. I asked why they were losing it. The operator (Dean Miller) said he didn't know.

I asked if they were using Oracle or a MS product. He said that it was a MS product and could be Foxpro or Access. He also said the system seemed busy while doing a look-up on it.

It would appear that there are either serious administrative problems or that there are software problems or both at this Microsoft branch. Likely the software problems are related to multi-user addition of records (there are multiple operators).

Does somebody know which database they are using and why the system doesn't work?

Please do not use the operator's name. Please allow me to see the final posting before using my name.

James Briggs, Toronto jeb@vigard.mef.org or CI\$ 71022,3700

C, MS Windows & dBASE consulting GPS(NAD27): N43o39.840' W079o22.701'+120m

Re: FireFly in the Ointment

<ark@whamr.att.com> Thu, 10 Feb 94 21:55:36 EST

This article (re: backwards accelerometers) reminds me of a story from my own

past. Years ago, I was writing a simulation of a guidance system. For some inputs, the output rate was in the wrong direction. So I traced through the equations and found the "erroneous" sign. This fixed the original problem, but created a similar problem along another axis. I changed the "wrong" sign in another equation, and presto, the problem moved to the third axis. I changed another sign, confident that I had the correct combination now. Instead, the problem now appeared on *two* axes. Any change I made in any equation just moved the bug elsewhere.

Well, after spending the better part of a day, I realized the true problem. I had reversed the sign of the acceleration due to gravity, so my program thought that the force of gravity pulled *up*. Once I corrected this, the program worked fine.

The moral: How about "Can't fool Mother Nature, or Mr. Newton"?

Andy Kostic ark@whamr.att.com

✓ Re: Firefly in the Ointment

Barbarisi <marco@email.ncsc.navy.mil> Fri, 11 Feb 1994 13:04:44 -0600 (CST)

Don Watts' letter describing the reversal of the Firefly control system, such that it flies in a direction opposite to that intended, is archetypical of navigation, guidance, and control systems.

Most such systems specify spatial conventions (i.e., which way is up) for the vehicle very early in the development, usually in the system specification. A competent system engineer will lay down the law that these conventions shall be followed now and forever and always. This is good. However, as the systems evolves from paper to actual hardware, it is found that some off-the-shelf subsystems do not conform to the spatial conventions established early in the program. Furthermore, costs to reconfigure such off-the-shelf items may appear prohibitive. This is bad.

An example might be an avionic inertial navigation unit which is adopted for use in an underwater vehicle. Is the altitude readout signed? Does depth correspond to negative or positive altitude? Maybe we could mount the inertial navigation unit up-side down - but no - that reverses pitch and yaw! By this time, the system engineer has that resigned, forlorn look of Gary Cooper in High Noon.

What about standards? There are standards for these things, but as someone on the net liked to point out, "The nice thing about standards is there are so many to choose from."

Marco Barbarisi

★ Re: Sounding the Alarm: Noisy medical alert systems

"Anthony E. Siegman" <siegman@Sierra.Stanford.EDU> Wed, 9 Feb 1994 21:49:51 -0800

Following the 1989 earthquake, all the fire and other hallway alarms in my one-story laboratory building at Stanford University went off and could not be stopped.

These alarms all in concert were so loud that in attempting to do a building check for possible fires, spilled chemicals, injuries in interior lab rooms and the like, I found it almost physically impossible to stay in the hallways, much less communicate audibly with others. Cries from possible victims, perhaps trapped under furniture or bookshelves in laboratory rooms, would have been totally impossible to hear. Emergency rescues or damage repair would have been greatly hampered.

There was no way to turn off these alarms; I was told that only the appropriate Public Safety personnel could do so, and that the staff in our building did not even know how or where to turn them off. Because necessarily every building on campus was in a similar situation, our alarms continued to operate for several hours before they could be turned off.

Fire alarm testing risks

Georg Feil <georg@sgl.ists.ca> Thu, 10 Feb 1994 16:31:39 -0500

The building where I work has its fire alarm system tested annually, in addition to possible fire drills. A few days ago the following email message was sent out to all occupants:

Xxxx Limited will be testing the Fire Alarm System on TUESDAY FEBRUARY 15, 1994 FROM 9:00 A.M. to 5:00 P.M. This is just going to be a test, so if you hear the bells ringing you do not have to evacuate.

There are at least two obvious risks, first of course that an actual fire on that day could be quite disastrous, and second the usual email risk that not everyone in the building that day will have seen the message, leading to confusion.

The capper came the next day when another email message was sent out:

The date for the fire alarm testing has been changed to Wednesday February 23rd from 9:00 to 5:00.

Talk about a perfect way to amplify a risk...

Georg Feil, Space Geodynamics Laboratory, Institute for Space and Terrestrial Science (416) 665-5458 georg@sgl.ists.ca

Re: Don't trust the phone company

Joe Konstan <konstan@cs.umn.edu> Thu, 10 Feb 1994 16:07:12 -0600

I've heard (on comp.dcom.telecom.tech) of several tricks that can be used to set up these situations. The two most common are:

- For caller-ID systems, there are devices that send another caller ID
 down the line after the phone call is answered. Somebody looking at
 the display would have to scroll backwards to find the "real" number, but
 would have no reason to know to do so.
- For automatic callback, as you describe, the obscene caller can forward the return call (along with any other calls) to a different number. In this case, if the obscene caller forwarded calls to your phone, the return would end up there.

Your subject is one of the lessons. Another is not to let the phone company off the hook for tracing obscene calls simply because they've provided a few technical features to the user.

Joe Konstan

Don't trust the phone company

<Spencer.W.Thomas@med.umich.edu>
Thu, 10 Feb 94 15:11:39 EST

A question: what does the "dial back" service do if the caller has suppressed caller-id with *70? Does it "wipe" the memory, or does it keep the number from the previous call?

Re: Don't trust the phone company (Bodine, RISKS-15.46)

<Michal.Jankowski@fuw.edu.pl> Thu, 10 Feb 94 23:17:57 +0100

Another possibility is that his wife had called your wife recently and he actually pressed `redial' on his phone instead of activating that `abuser-combating feature'. It's easy to misdial some keys when you are angry.

Michal.Jankowski@fuw.edu.pl

★ Re:Don't trust the phone company (Bodine, RISKS-15.)

Nancy Griffeth <nancyg@banshee.bellcore.com> Thu, 10 Feb 1994 22:30:44 GMT

This is an interesting and disturbing story. You have probably been the

victim of either a feature interaction or a bug in the implementation of the code that updates the calling number.

I've been following the discussion of this problem on the Telecomm Digest, and most of the possibilities have been listed there:

To summarize:

Possibility 1: The calling number from the obscene call was not updated because for some reason it wasn't delivered to Tom's central office. The register still contained the Tom's number, from an earlier call placed by his wife.

Possibility 2: Another feature (possibly call waiting) interfered in such a way that Tom's number replaced the number of the obscene caller.

Possibility 3: The obscene caller was clever enough to call-forward his or her phone to Tom's number immediately after ending the obscene call. This is an unpleasant thought, since it suggests that he or she knows Tom or his wife and is actively trying to make trouble.

Tom, you should tell your friend, or is it your wife's friend's husband, that any one of these could have happened.

The first possibility is almost certainly a bug -- Bellcore writes requirements for these features, and its requirements say that the number should always reflect the last caller unless the last caller received busy or call forwarding treatment. On the other hand, Bellcore doesn't write switching software, and the companies that write it don't have to follow the requirements exactly. So it may not even be a bug, it may have been the way that AT&T or NT or whoever wanted it to work.

The second possibility could have happened if your wife's friend has call waiting, and your wife called her after the obscene call began, and her friend was sufficiently distracted by the call not to notice the call waiting. Then your number would have been used by automatic recall, at least according to Bellcore specifications.

The third possibility means that the return call went initially to the obscene caller, but was routed to you by call forwarding. Recommending that your wife's friend get Calling Number Delivery won't help -- if an obscene caller is clever enough to do the call forwarding right after the call, he has already blocked Calling Number Delivery. On the other hand, there's yet another feature, Call Origination Trace, that may be useful. I can't find the documentation for it right now, but if I remember correctly you enter a code immediately after hanging up and the caller is reported to the police. Tell your wife to suggest to her friend that they try it.

Nancy Griffeth nancyg@bellcore.com

P.S. For anyone interested in more detail, here are the responses that appeared on Telecom Digest:

Possibility 1: The calling number from the obscene call was not updated

because for some reason it wasn't delivered to Tom's central office. ...

- <>From: rhorer@medics.jsc.nasa.gov (Kyle Rhorer)
 <>Is it possible that Mrs. Bodine was the last caller *before*
 <>the obscene call, and the obscene call came from a subscriber in a
 <>different operating company? Perhaps the OC that serves the Bodines
- <>simply doesn't update the call return register if the call is from an
- <>"unidentifiable" source?
- <>
- <>
- <>[TELECOM Digest Editor's Note: I don't think this is true. I think the
- <>buffer which holds that information is flushed each time around, meaning
- <>valid, identifiable information from an earlier call would be erased by
- <>the new call, even if the new call put nothing more than 'outside' or
- <>'cannot identify' in the buffer where the previous information had been. PAT]

and also:

- <>From: Monty Solomon <monty@roscom.COM>
- <>Call Return works only for calls which originate in areas which have
- <>the availability of the PHONESMART package (Caller ID, Call Return,
- <>Repeat Dialing, and Call Trace).
- <>
- <>[TELECOM Digest Editor's Note: What seems to put a fly in the ointment
- <>where the arguments about false identification due to a variety of
- <>possible causes (one call arrived when line was busy, next call went
- <>in the 'return call' buffer, etc, call returned to the wrong party of
- <>the two who called about the same time) is Mr. Bodine's comment that
- <>this woman had received *several* obscene calls over a period of time.
- <>Surely the intricacies of the modern phone network did not interact
- <>in such a bizarre way every time. If there have been so many obscene
- <>calls, can't the woman at least identify the voice of the caller, or
- <>listen to Mr. Bodine's voice and qualify or disqualify him as the
- <>person responsible? PAT]

Comments: Kyle, Monty, and Pat are both right in a way.

In favor of Pat's point: The Bellcore requirements state that if the calling number is not available, the register that holds the calling number should be updated in such a way as to reflect its unavailability. To quote from the LSSGR Feature Specification Document FSD 01-02-1260 on the subject of Automatic Recall (Bellcore's name -- the name varies from region to region and country to country):

The AR feature enables a customer to place a call to the last station that called the customer and did not receive busy or call forwarding treatment.

In favor of Monty's and Kyle's points: Bellcore doesn't write switching software; almost all switching software used in the US is written by AT&T or NT. Bellcore requirements are more suggestions than real requirements... so, does Tom's particular switch (which may be any one of several AT&T or NT switches) actually do the updating as recommended by Bellcore? It's

quite possible that it doesn't. And two different switches may do different things!

Pat's argument that coincidences couldn't have caused this problem every time is irrelevant, though, because Tom was talking about just *ONE* callback, immediately after his friends had bought the service. The point he was making was that his friends bought the service because they had received a number of obscene calls.

Possibility 2: Another feature (possibly call waiting) interfered in such a way that Tom's number replaced the number of the obscene caller.

<>From: brena@sol.aa.hcia.com (Brian D. Renaud)
<>Lars Poulsen (lars@eskimo.CPH.CMC.COM) wrote:
<>
<>> I believe that there is no such interaction problem in the case of the
<>> "calling number identification" feature, since the number is delivered
<>> in real time and only when the call rings through. Thus, the call that
<>> would come in DURING the problem call, would only be recorded if the
<>> recipient had the "call waiting" feature, and in that case would not
<>> get busy, but ringback, and the CNID (if subscribed) would be delivered
<>> between the rings (call waiting tones)).
<>
<>In my experience, CNID is not delivered if your phone is busy, even if

<> <>Brian

<>you have call waiting.

<> <>

<>[TELECOM Digest Editor's Note: You are correct, it is not delivered if <>your line is busy, and it is only delivered (if arriving via call waiting) <>on one condition that I can determine: if the call-waiting party stays on <>the line, allowing it to ring, then when the called party and whoever he <>is talking to disconnect the call-waiting call will start to ring through <>and Caller-ID will be delivered between the first and second audible <>rings heard by the called party just as though it was the first and second <>'true rings'. That is to say, you ring me and I am on a call. I get the <>call-waiting signal and tell my party we have to ring off so I can take <>the new call. We chat a few seconds more and hang up. Rather than flashing <>to accept the new call, I actually hang up and let my phone ring a couple <>times more. Between the first and second rings *that I hear* my display <>will get the Caller-ID, even if the calling party had to sit for a dozen <>rings or more. I'm not sure, but I think if I flash to answer, then put <>the party on hold and later hang up (the first call) allowing 'reminder <>rings' to tell me about the party on hold, I'll get Caller-ID between the <>first and second of those 'reminder rings' also. I know the first instance <>is correct; I think the second one is. That seems to be the one and only <>way of receiving Caller-ID under the circumstances: you have to hang up <>on the party you are talking with and let the call-waiting actually cause <>your phone to ring so delivery can be made to your display, regardless of <>how long that may be (or how many rings have occurred) since the call-<>waiting party entered your premises. PAT]

Whew! Well, Pat's wrong, and Lars has it right, if we look believe the Bellcore requirements. On the other hand, the implementation could be different.

Details of how the register is actually updated are given in Appendix E of Bellcore feature specification document FSD 01-02-1260 on Automatic Recall. As Lars said, customers that are call waited DO NOT receive busy treatment -- instead they get ringing. Appendix E specifies that "The incoming memory slot should always be updated for all incoming calls that are call waited, whether or not the incoming call is answered by the called party."

Pat is right about actual delivery of the Calling Number, but he is wrong to assume that this means the register is not updated. Even for Calling Number Delivery (or Caller ID), the register is updated when a caller is call-waited. It's not actually delivered to your phone because the signal is delivered in-band and delivering the number in the middle of a call would also deliver an ugly noise to your ear. There are proposals, however, for muting the sound briefly to deliver it. After all, often the only thing you want to know when you're already on the line is who's calling, so you can call them back.

Possibility 3: The obscene caller was clever enough to call-forward his or her phone to Tom's number immediately after ending the obscene call. This is an unpleasant thought, since it suggests that he or she knows Tom or his wife and is actively trying to make trouble.

```
<>From: Ben Burch <Burch_Ben@msmail.wes.mot.com>
<>
<>In article <telecom14.69.1@eecs.nwu.edu> TELECOM Digest Editor noted
<>in response to Lars Poulsen, lars@eskimo.CPH.CMC.COM:
<>
<>> ... If Mr. Bodine insists he is not the party who made the obscene
<>call, then I guess we take his word for it and find someone else to
<>blame; but it seems quite a stretch of the imagination ...
<>
<>Well ... I hope you'll take *my* word for this, too!
<>
<>About six, maybe seven months ago, I was sleeping, and was awakened by
<>the telephone ringing:
<>Me: "Good evening, Burch residence"
<>
<>Female Caller: "Who is this?"
<><moment of disorientation, non-sequiturs at 1:00 AM cause this ...>
<>
<>Me: "I think I ought to ask you that, since you called me..."
<>
<>FC: "No, *you* called me."
<>
<>Me: "The telephone was ringing, and I answered it, so, really, I'm pretty
```

```
<>sure you called me."
<>
<><this was starting to sound like some bad practical joke.>
<>FC: "No, you made an obscene call to this number just now, and I used
<>call return to call you back."
<>Me: "I'll beg your pardon, but there is nobody at this number but me at
<>present, and I was sleeping."
<>
<>FC: "If you ever call me again, I'll see you arrested." *click*
<>So, I'm absolutely *certain* that there are major bugs with this
<>feature. Possibly some bright jerk has figured out how to give it
<>false information, but I'd bet on a bug first. (I've done telephone
<>switch programming, so I'm allowed to have an opinion ...)
<>
<>
<>Ben Burch Motorola Wireless Data Group Ben Burch@msmail.wes.mot.com
<>
<>
<>[TELECOM Digest Editor's Note: Oh, I believe you. It could be that
<>whoever called the lady quickly call-forwarded his line to yours
<>immediately after disconnecting; he woke her up with his call, she sat
<>there in a just-awakened stupor and thought about it for a minute then
<>used 'return last call' to reach you via him. This is where having
<>Caller-ID *and* 'return last call' both on the line would be useful.
<>That way one could see the actual number placing the call even if the
<>return trip led somewhere else. Maybe there ought to be a dialing code
<>for the purpose of 'do not forward'. That is, the person placing the
<>call would dial some two-digit code (such as for blocking or do not
<>disturb) which meant 'absolutely ring number such and such'. This would
<>be sort of like the post office endorsement we can use on letters which
<>says, 'do not forward, return to sender if unable to deliver as addressed'.
<>Telco's response would be to ring that number or respond with a voice
<>intercept, 'cannot ring that number now' if the number was being for-
<>warded. There may be times, for example, when I wish to speak with you
<>but not if I know you are elsewhere; in those cases I am willing to wait
<>until you are at home. The recipient's Caller-ID box would show some
<>notation such as 'forced delivery from xxx-yyyy' to indicate a call had
<>been received but not forwarded at the caller's request. PAT]
```



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 54

Monday 14 February 1994

Contents

- Info on RISKS (comp.risks)
- Voice-mail phreaking

Mich Kabay

Electronic Food Stamps

Mich Kabay

- Another ATM "front end" fraud this time caught Jonathan Haruni
- [Lighter Side] Risks of computer-literate babies Robert J Woodhead
- New Novel/Thought experiment...

Peter Wayner

Recent Articles of Interest

Bob Frankston

Re: Celebrity Risks -- Bill Gates

John Bush

Card Fraud and Computer Evidence

Ross Anderson

Voice-mail phreaking

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 14 Feb 94 03:20:52 EST

Hacker attempts to chase cupid away

SAN FRANCISCO (UPI, 10 Feb 1994) -- Two bachelors who rented a billboard to find the perfect mate said Thursday they had fallen victim to a computer hacker who sabotaged their voice mail message and made it X-rated. Steeg Anderson said the original recording that informed callers how they may get hold of the men was changed to a "perverted" sexually suggestive message. He said the tampering occurred sometime Wednesday." [United Press newswire via Executive News Service (GO ENS) on CompuServe]

The article states that Pacific Bell has been investigating other voice-mail tampering recently as well.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Electronic Food Stamps

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 14 Feb 94 03:21:03 EST

Welfare Cards (By Michael Holmes, Associated Press Writer)
AUSTIN, Texas (AP, 10 Feb 1994) -- Texas plans to begin providing welfare benefits electronically this year with bank-style cards that take the place of paper coupons. The new system is designed to reduce administrative expenses, fraud and theft. [From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe]

The author continues with the following key points:

- o "Electronic benefits transfer" will begin in two counties in autumn 1994 and should be statewide by 1996.
- o The Lone Star Card will function like a debit card, allowing holders to purchase food only in cooperating grocery stores.
- o Cardholders will use a 4-digit PIN.
- o Officials hope the cards will reduce fraud by eliminating all cash from food-stamp transactions (sometimes stores returned change).

It will be interesting to watch this program to see how security aspects are handled.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Another ATM "front end" fraud - this time caught

Jonathan Haruni <jharuni@london.micrognosis.com> 14 Feb 1994 10:23:30 GMT

An Article in London's Evening Standard of February 11 says that "in one of the most ingenious and innovative high-tech crimes of recent years", culprits planted a fake ATM card reader at a London branch of the Midland bank. In a variation on the theme, the reader was not planted over top of the ATM, but was installed to emulate the door opening devices which most banks use. Users were asked to swipe their cards through the device, and then type in their PINs, to gain admission to the ATM hall.

A suspicious customer informed the bank. Some customers had used the device unsuspectingly, but no money was stolen.

I see the following developments:

- As we know, thieves are well able to reproduce magnetic swipe cards. They no longer need to steal peoples' cards to gain access to their accounts. Any scheme which gives the card number and PIN will do. If this plan really qualified as "ingenious" it would have transmitted the data by radio directly to the thieves' card making machine, and the resulting cards would have been used without delay.
- The article was on the front page of a popular newspaper. Although it did contain some excess verbiage (such as the quote above) it also contained all the salient technical details, it described the extent of success and the outcome of the scheme. There is a quote from a bank spokesman and a quote from the police.

I've never seen such a complete description of a RISK-worthy story in such a prominent position. Is this a sign that the non-technical public are becoming more aware of the risks of technology, or at least more interested in it?

Jonathan Haruni

[Lighter Side] Risks of computer-literate babies

Robert J Woodhead <trebor@foretune.co.jp> Tue, 15 Feb 1994 09:07:29 +0900

My wife and I are blessed with an extremely literate 14-month-old boy. James is extremely enamoured of technology in general, with special attention being given to remote controls and our family Powerbook laptop.

As you might expect, we suffered through the usual baby-instigated data processing disasters (leave the Mac unattended for a moment and he'll go and click the mouse or hit keys in such a way as to maximize the damage), but we have since adjusted to these dangers.

Yesterday, however, he got us but good. In a display of hitherto unsuspected manual dexterity, he managed to introduce into the floppy disc drive a used popsicle stick, a fact not discovered until some time later when an attempt was made to insert a floppy into the drive.

15 minutes and a spirited display of vocabulary on the part of this author later, the errant splinter was removed with the help of a bent paperclip. In a tribute to modern floppy disc design, the drive has apparently survived the introduction of wood pulp and traces of raspberry juice.

The risks are of course obvious. As our children become more and more computer literate at an earlier age, we need to develop a new BABYSPEC specification (similar to MILSPEC but tougher), which should include (but not be limited to)

* Diskette drive flaps that only flap for real diskettes.

- * Hardened keyboards capable of withstanding two-fisted infant impacts (our "f" key will never be quite the same, though we did manage to get it working again with a paperclip).
- * Smudge-resistant screens.
- * Washable.
- * And, of course, a baby-proof paperclip storage area.

Robert J. Woodhead, Biar Games / AnimEigo, Incs. trebor@forEtune.co.jp |

New Novel/Thought experiment...

Peter Wayner <pcw@access.digex.net>
12 Feb 1994 18:46:50 -0500

If you're interested in a thought experiment about how to abuse the Intelligence system and products like Clipper, then read Joe Finder's new novel, _Extraordinary Powers_ (Ballentine). It's a great spy novel/technothriller that kept me up long past my bedtime. Saying anymore would spoil the story. (I should say that he is a friend...) Peter

Recent Articles of Interest

<Bob_Frankston@frankston.com> Mon, 14 Feb 1994 00:26 -0400

I won't attempt to do more than a very brief comment on each one. As I've noted in the past, some of us (would like to) assume that simply placing a reference (link) should sufficient. In the world of the Web it's actually starting to happen.

Discover Magazine (March 1994) has an article entitled "Counting on Dyscalculia" (which I've called innumeracy). It discusses various problems familiar to Risks readers such as the fact that a false positive rate on a rare disease produces results which are not very good indicators of whether you have the disease. It mentions the impact on public policy such as banning substances at levels that are a fraction of what we ingest anyway.

A recent issue of Science News (which I put aside to mention here and have yet to find again) summarizes research on the difference between logical reasoning and human reasoning. In many cases humans reason correctly. These are the cases that make sense to the person doing the reasoning. Otherwise they can be very far off. It covers some of the open issues such as how much people use correlation and coincidence because of its evolution advantages in the absence of complex reasoning. Again, not a surprising article for Risks readers. It does jibe with my observation phrase like "Couldn't care less" and "could care less" mean the same thing because the sentence is analyzed against one's own semantic biases as opposed to logical analysis.

The Feb. 13th Sunday New York Times had two articles. One is by Peter Lewis based on the CERT alert. It has a sidebar illustrating how a Kerberos challenge/response key system works. Lawrence Fisher has an article on the

changes in Telecommuting since the San Francisco earthquake. It says that security is a serious concern and has some discussion on approaches.

Re: Celebrity Risks -- Bill Gates

John Bush <jbush@access.digex.net> Mon, 14 Feb 1994 18:48:48 -0500 (EST)

In RISKS-15.53, Jack B. Rochester writes:

> The Jan. 10, 1994 issue of The New Yorker has a long, juicy article entitled > "E-Mail From Bill,"

And NOW, from the 21 Feb 1994 issue of BusinessWeek:

BILL GATES INUNDATED IN BOX

A personality profile in _The New Yorker_ magazine's Jan. 10 issue revealed Bill Gates's electronic-mail address -- and his electronic in box hasn't been the same since. "I've got 5,000 messages stacked up," says Gates, CEO of the Redmond (Wash.) giant, Microsoft. That's up from no more than 10 e-mail messages daily before from the outside (although he may receive as many as 250 per day internally).

Until the article ran, the software billionaire was never too busy to read -- and often respond to -- messages sent from around the world via the Internet data highway. Gates chats with outsiders on items that include technology and business opportunities. In his email -ure of the Information Superhighway and his analysis of F. Scott Fitzgerald's _The Great Gatsby_. [This article has been taken verbatim from the magazine. I assume that last sentence is a misprint?]

Now, though, he has been forced to use a software program that sifts through the deluge to identify items from important people such as Intel CEO Andrew Grove. But what about the thousands of notes from who-knows-who that continue to stream in and sit in computer memory, ungraced by Bill's attention? Gates has never had anyone else read his electronic mail for him, "but I'm seriously considering it now."

..End of article.

If I remember correctly, that address is "billg@microsoft.com"...

CARD FRAUD AND COMPUTER EVIDENCE

<Ross.Anderson@cl.cam.ac.uk> Mon, 14 Feb 1994 13:15:28 GMT

A case has just concluded in England which may be significant for computer and cryptographic evidence in general, and for electronic banking in particular. It also give some interesting insights into the quality assurance and fraud

investigation practices of one of Britain's largest financial institutions.

I will be talking about this case to the BCS Computer Law Special Interest Group on Thursday 17th February at 6pm. The meeting will be held at the offices of Bristows Cooke Carpmael, which can be found at 10 Lincoln's Inn Fields. To get there, take the tube to Holborn, exit southwards and turn second left into Remnant Street.

For the sake of those who cannot make it, there follows a report of the case from the notes I made during the hearing.

* * *

1. Background.

On February 8th, 10th and 11th, I attended the trial at Mildenhall Magistrates' Court, Suffolk, England, of a man who was charged with attempting to obtain money by deception after he complained that he had not made six of the automatic teller machine transactions which appeared on his statement.

The essence of the case was that John Munden, a police constable, had complained to the manager of the Halifax Building Society in Newmarket about these transactions, which appeared in September 1992. He had also stated that his card had been in his possession at all times. Since the society was satisified about the security of its computer systems, it was alleged to follow that Munden must have made these transactions, or suffered them to be made; and thus that his complaint was dishonest.

This trial had resumed after being adjourned in late 1993. According to the clerk, evidence was given for the Crown at the initial hearing by Mr Beresford of the Halifax Building Society that the society was satisfied that its systems were secure, and so the transaction must have been made with the card and PIN issued to the customer. Beresford had no expert knowledge of computer systems, and had not done the investigation himself, but had left it to a member of his department. He said that fraudulent transactions were rarely if ever made from lobby ATMs because of the visible cameras. The Newmarket branch manager, Mr Morgan, testified that one of the transactions at issue had indeed been made from a machine inside the branch. He also said that in his opinion the defendant had been convinced that he had not made the transaction; and that he would not be aware of all the possible malfunctions of the ATM.

The defence had objected that the evidence about the reliability of the computer systems was inadmissible as Beresford was not an expert. The court allowed the prosecution an adjournment to go and look for some evidence; and at the last minute, on the 20th January, I was instructed by Mr Munden's solicitor to act as an expert witness for the defence.

2. The Prosecution Case.

On 8th February, Beresford's evidence resumed. He admitted that the Halifax had some 150-200 'unresolved' transactions over the previous 3-4 years, and that it would be possible for a villain to observe someone's PIN at the ATM and then make up a card to use on the account. He confirmed that the person who investigated the incident had no technical qualifications, had acted under

his authority rather than under his direct supervision, and had involved the police without consulting him.

Evidence was next given by Mr Dawson, the Halifax's technical support manager. He had originally written the bank's online system in 1971, and was now responsible for its development and maintenance. The ATM system had been written in 1978 for IBM 3600 series machines, and altered in 1981 when the Diebold machines currently in use were purchased. All software was written internally, and in the case of the mainframe element, this had accreted to the nucleus originally written in 1971. Amendments to the online system are made at the rate of 2-3 per week.

The PIN encryption scheme used was nonstandard. The PIN was encrypted twice at the ATM and then once more in the branch minicomputer which controls it. At the mainframe, the outer two of these encryptions were stripped off and the now singly encrypted PIN was encrypted once more with another key; the 16 digit result was compared with a value stored on the main file record and on the online enquiry file.

When asked whether system programmers could get access to the mainframe encryption software, he categorically denied that this was possible as the software could only be called by an authorised program.

When asked whether someone with access to the branch minicomputer could view the encrypted PIN, he denied that this was possible as there were no routines to view this particular record (even although the mini received this field and had PCs attached to it). When asked what operating system the mini used, he said that it was called either TOS or TOSS and that he thought it had been written in Sweden. He could give no more information.

He had never heard of ITSEC.

He had not investigated any of the other 150-200 'unresolved transactions' because he had not been asked to. The last investigation he had done was of another transaction which had led to a court case, three years previously; he had no idea what proportion of transactions went wrong, was not privy to out-of-balance reports from branches, and was not familiar with branch rules on ATM operations. He never visited the branch at Newmarket, where the disputed transactions took place, but merely looked at the mainframe records to see whether any fault records or error codes. He found none and took this information at face value.

The fault recording system does not show repairs. The cryptographic keys in the ATM are not zeroed when the machine is opened for servicing. The maintenance is done by a third party. The branch only loads initial keys into the ATM if keys are lost.

The Halifax has no computer security function as such, just the internal auditors and the technical staff; it does not use the term 'quality assurance'.

When asked by the bench what information was required to construct a card, Dawson initially said the institution identifier, the account number, the expiry date, a service code, an ISO check digit, a proprietary check digit,

and a card version number. He concluded from this that a card forger would have to have access to an original card. However it turned out that the ATM system only checks the institution identifier, the account number and the card version number. He maintained doggedly that a forger would still have to guess the version number, or determine it by trial and error, and claimed there was no record of an incorrect version number card being used.

However, Munden's card was version 2, and it transpired later that version 1, though created, was not issued to him; and that an enquiry had been made from a branch terminal two weeks before the disputed transactions (the person making this enquiry could not be identified). When asked whether private investigators could get hold of customer account details, as had been widely reported in the press, he just shrugged.

He claimed that the system had been given a clean bill of health by the internal and external auditors.

The branch manager was recalled and examined on balancing procedures. He described the process, and how as a matter of policy the balancing records were kept for two years. However the balancing records for the two machines in question could not be produced.

There was then police evidence to the effect that Munden kept respectable records of his domestic accounts, which included references to the undisputed withdrawals from ATMs, and that although he had once bounced a cheque he was no more in financial difficulty than anybody else. The investigating officer had only had evidence from the branch manager, not from Beresford or Dawson. The investigating officer also reported that Munden had served in the police force for nineteen years and that he had on occasion been commended by the Chief Constable.

3. The Defence.

That concluded the prosecution case, and the defence case opened with Munden giving evidence. He denied making the transactions but could not produce an alibi other than his wife for the times at which the alleged withdrawals had taken place.

The only unusual matter to emerge from Munden's testimony was that when he went in to the branch to complain, the manager had asked him how his holiday in Ireland went. Munden was dumbfounded and the branch manager said that the transaction code for one of the ATM withdrawals corresponded to their branch in Omagh. This was not apparent from the records eventually produced in court.

The next witness was his wife, Mrs Munden. Her evidence produced a serious upset: it turned out that she had had a county court judgment against her, in a dispute about paying for furniture which she claimed had been defective, some two weeks before the disputed withdrawals took place. Her husband had not known about this judgement until it emerged in court.

I gave expert evidence to the effect that the Halifax's quality procedures, as described by Dawson, fell far short of what might be expected; that testing of software should be done by an independent team, rather than by the programmers and analysts who created it; and that Dawson could not be considered competent

to pronounce on the security of the online system, and he had designed it and was responsible for it.

At a more detailed level, I informed the court that both national and international ATM network standards require that PIN encryption be conducted in secure hardware, rather than software; that the reason for this was that it was indeed possible for system programmers to extract encryption keys from software, and that I understood this to have been the modus operandi of a sustained fraud against the customers of a London clearing bank in 1985-6; that I had been involved in other ATM cases, in which some two dozen different types of attack had emerged and which involved over 2000 complaints in the UK; and that the Halifax, uniquely among financial institutions, was a defendant in civil test cases in both England and Scotland.

I continued that ATM cameras are used by a number of other UK institutions, including the Alliance and Leicester Building Society, to resolve such cases; that in other countries which I have investigated the practice would be not to prosecute without an ATM photograph, or some other direct evidence such as a numbered banknote being found on the accused; that card forgery techniques were well known in the prison system, thanks to a document written by a man who had been jailed at Winchester some two years previously for card offences; that I had personally carried out the experiment of manufacturing a card from an observed PIN and discarded ticket, albeit with the account holder's consent and on an account with Barclays rather than the Halifax; that the PIN pad at the Halifax's Diebold ATM in Cambridge was so sited as to be easily visible from across the road; and that in any case the investigative procedures followed in the case left very much to be desired.

In cross examination, the prosecutor tried to score the usual petty points: he attacked my impartiality on the grounds that I am assisting the Organised Crime Squad at Scotland Yard to investigate criminal wrongdoing in financial institutions (the reply from our lawyer was of course that helping the prosecution as well as the defence was hardly evidence of partiality); he claimed that the PIN pad at the ATM in Newmarket was differently sited to that in Cambridge, to which I had no answer as I had not had the time to go there; and he asserted that the Alliance and Leicester did not use ATM cameras. On this point I was able to shoot him down as I had advised that institution's supplier. He finally tried to draw from me an alternative theory of the disputed transactions - staff fraud, or a villain whom Munden had booked in the past getting his own back by means of a forged card, or a pure technical glitch? I was unable to do this as there had been neither the time nor the opportunity to demand technical disclosure from the Halifax, as had been the case in two previous criminal cases I had helped defend (both of which we incidentally won).

Dawson was recalled by the prosecution. He explained that only two of the three tests carried out on new software were done by the analysis and programmers who had written it, and that the third or 'mass test' was done by an independent team. He said that software failures could not cause false transactions to appear, since the online system was written in assembler, with the result that errors caused an abend.

He claimed that they did indeed possess a hardware security module, which was

bought in 1987 when they joined VISA, and which they used for interchange transactions with VISA and Link although not for all transactions with their own customers; and he finally repeated his categorical denial that any system programmer could get at the encryption software. When asked by what mechanism this was enforced, he said that they used a program called ACF2.

In his closing speech, the defendant's lawyer pointed out the lack of any apparent motive, and went on to point out the lack of evidence: the balancing records were not produced; the person responsible for attending to those ATM malfunctions which the branch could not cope with was not identified; the Halifax employee who had carried out the investigation was not called; the handwriting on the ATM audit rolls, which was the only way to tie them to a particular machine, could not be identified; the cameras were not working; statements were not taken from branch staff; the disk in the ATM had not been produced; and the internal and external audit reports were not produced.

He mentioned my expert opinion, and reiterated my point that when a designer of a system says that he can't find anything wrong, what has he shown? He also recalled that in the High Court action in which the Halifax is the defendant, they had not relied on the alleged infallibility; and pointed out that if ATM systems worked properly, then people wouldn't need to go to keep going to law about them.

4. The Verdict and Its Consequences.

I have been aware for years that the legal system's signal-to-noise ratio is less than 10dB; however, in view of the above, you can understand that it was with some considerable surprise that I learned late on Friday that the court had convicted Munden. My own reaction to the case has been to withdraw my money from the Halifax and close my account there. Quite apart from their ramshackle systems, the idea that complaining about a computer error could land me in prison is beyond my tolerance limit.

No doubt it will take some time for the broader lessons to sink in. What is the point, for example, of buying hardware encryption devices if people can get away with claiming that system programmers can never get at an authorised library? Why invest in elaborate digital signature schemes if they simply repair the banks' defence that the system cannot be wrong? Is there not a case for giving more consideration to the legal and political consequences of computer security designs?

5. Action.

In the meantime, the police investigations branch have to consider whether John Munden will lose his job, and with it his house and his pension. In this regard, it might just possibly be helpful if anyone who feels that Dawson's evidence was untruthful on the point that software can be protected from system programmers on an IBM compatible mainframe, or that his evidence was otherwise unsatisfactory, could write expressing their opinion to the Chief Constable, Cambridgeshire Constabulary, Hinchingbrooke Park, Huntingdon, England PE18 8NP.

Ross Anderson



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 55

Tuesday 15 February 1994

Contents

- YAMIC [Yet Another Mistaken Identity Case] Robert Herndon
- William Safire on Clipper: ESSAY: SINK THE CLIPPER CHIP **PGN**
- Over 10,000 Sign Petition to Oppose Clipper Dave Banisar
- Canada to monitor phone calls,fax,etc.? Sahel Allevasin
- No switch on new Sun Microphone Olin Sibert
- Electronic Mail vs Paper Mail mathew
- FIRP report comments Stephen D Crocker
- Info on RISKS (comp.risks)

✓ YAMIC [Yet Another Mistaken Identity Case]

Robert Herndon <rh@craycos.com> Tue, 15 Feb 94 14:50:59 MST

Excerpted from the Minneapolis Star and Tribune, Sunday, Feb. 13, 1994.

THE RIGHT NAME, THE WRONG MAN

Freed after a month in jail, innocent man found he'd lost job, van, and girlfriend. By Margaret Zack, Staff Writer

Maintenance worker Russ Hamilton tried for more than a month to convince authorities that he wasn't truck driver Russ Hamilton, who was wanted for fraud. His troubles began Nov. 28 at a Salt Lake City party that got out of hand. Police were called, and Hamilton was arrested on two misdemeanor charges. In a routine check, police found there was a warrant out for a Russell Hamilton in Wisconsin, and both men had the same birth date. So

Hamilton sat in jail.

... Dane County deputies flew to Salt Lake City and took him to Wisconsin on Dec. 19. He remained jailed, always protesting his innocence, until Dec. 30, when authorities learned they had the wrong man and released him. ... the evidence that freed him -- a photo of the man wanted on the fraud charges -- had been in the prosecutor's file all along.

Hamilton, and his attorney Alan Albrecht of Brooklyn Center, said last week that someone had obtained Hamilton's birth date and gotten a driver's license in his name. They said they don't know how that occurred. The fraud suspect has reportedly been identified but is not in custody.

What Albrecht finds so appalling about the case is that the photo of the real person wanted in Wisconsin was always in the prosecutor's file. "The picture could have been faxed out to Salt Lake City," he said. Or at least the deputies who flew to Utah could have taken the photo with them to be sure they had the right suspect, he said.

... But the prosector told him those would have been "extraordinary" measures and weren't warranted in the case, Albrecht said. The Dane county prosecutor who handled the case did not return repeated phone calls last week.

[The article goes on to detail differences between Hamilton and the man wanted for fraud: Hamilton is 37, 5'9", heavy, with long hair, a goatee, and tattoos on his arms. The man wanted for fraud is over 6' tall, thin, and in his 50s.

In addition, while Hamilton was in jail, authorities seized his van and its contents and sold them. His girlfriend, with whom he shared an apartment, moved out, and he hasn't been able to locate his clothes, furniture, or other possessions. He is now living in Minneapolis with a brother, and is preparing a civil lawsuit.

The risks of technology here are apparent and familiar to RISKS readers. In this case, too, technology would seem able to have provided reasonable safeguards. That a simple check would be regarded as "extraordinary" seems itself extraordinary, but alas, is all too common.

[Here is a case where checking the SSN might have helped -- except that the RISKS archives contain several cases of two people with the same name who were accidentally assigned the same SSN! PGN]

★ William Safire on Clipper: ESSAY: SINK THE CLIPPER CHIP

"Peter G. Neumann" <neumann@csl.sri.com> Tue, 15 Feb 94 10:40:52 PST

The Op-Ed page (A13) of the National Edition of The New York Times on 14 Feb 1994 had a piece by William Safire that is worth ferreting out. Three paragraphs (excerpted out of 15) summarize his message:

To the tune of ``I Got Algorithm," the Eavesdrop Establishment is singing that it will help us protect our privacy but not from intrusion by the Feds. In effect, its proposal demands we turn over to Washington a duplicate set of keys to our homes, formerly our castles, where not even the king in olden times could go.

Tomorrow's law enforcement and espionage cannot be planned by people stuck in the wiretap and Big Ear mind set of the past. The new Ultra secret is that the paradigm has shifted; encryption has overcome decryption.

Cash in your clipper chips, wiretappers: you can't detect the crime wave of the future with those old earphones on.

✓ Almost 15,000 Sign Petition to Oppose Clipper

Dave Banisar <cpsr@access.digex.net> Tue, 15 Feb 1994 13:42:29 -0500

Washington, DC
February 15, 1994 (second edition)
Computer Professionals for Social Responsibility (CPSR)
ALMOST 15,000 HAVE SIGNED PETITION TO OPPOSE CLIPPER

In only two weeks, almost 15,000 users of the nation's computer networks have signed the CPSR petition calling for President Clinton to withdraw the Clipper proposal. Opposition has been widespread, from CEOs of large firms to college students in small towns, from librarians and civil libertarians to computer programmers and product marketers.

To sign the petition, email <clipper.petition@cpsr.org> with the message "I Oppose Clipper". [See Banisar, RISKS-15.44 for the petition. PGN]

In 1990, over 30,000 people sent email message to Lotus asking that a product containing detailed personal information called "Marketplace" be withdrawn. Eventually Lotus withdrew the product.

CPSR is a non-profit, membership organization based in Palo Alto, CA. CPSR's mission is to provide analysis of the effects of new technological developments on society. For more information, please email cpsr@cpsr.org or call 415-322-3778.

[MODERATOR's NOTE: Many contributions have been received on escrowed keys, Clipper, et al. Some are repetitions of what has already been included, others are full of ad hominem comments and not appropriate for RISKS. There are also some messages that are lengthy interstitiations of already too-long messages. You will all appreciate that I am having to moderate much more stringently than usual. But the overwhelming majority of E-mail is opposed to EES/Clipper, and in support of the CPSR petition. PGN]

Canada to monitor phone calls, fax, etc.?

Sahel Alleyasin <eng350q3@csulb.edu> 15 Feb 1994 23:41:17 GMT

Canadian security intelligence services is trying to make equipment to keep records of all conversations from millions of airborne phone, fax, radio signal and other transmissions.

The first thing that comes to my mind from this high-tech snoop gadget is that it violates the people's trust and confidence. Nobody can ever be confident to have a private conversation with others. They are always afraid of what have been said because the government keeps records of these conversations. This monitoring of phone calls is the invasion of privacy.

As we have read from the other examples in the text book about risk_forum digest contributions, the computers could make mistakes. In the case of Canadian government, using computers could cause someone else to be accused by the government for something he/she didn't do. An error could result, for example, from two persons having the same name.

The other risk factor could be the possibility of an intruder accessing a system and erasing some of the data or other information. An intruder changing the data could cause other people to be at risk.

Computers are not always to be credited. They could make errors, or someone else could cause these errors by changing the data. This hardware on Canadian security service will have the same problem, but the main issue is that the Canadian government is taking advantage of the new technology to invade people's private life.

No switch on new Sun Microphone

Olin Sibert <wos@oxford.com> Tue, 15 Feb 94 09:47:11 EST

A recent product announcement from Sun Microsystems (SunFLASH Vol 62 #8, 4 February 1994) introduces "new microphone, SunMicrophone II, to ship with current and new Sun desktop platforms". Among the features described by the announcement for this "uni-directional microphone which allows greater focus on direct voice input while providing less interference from background ambient noise" is the following Q&A:

- Q. Does the SunMicrophone II look similar to the SunMicrophone?
- A. No, the two products look very different. The current SunMicrophone has a unique square shape, with an on/off switch. The SunMicrophone II looks like a classic microphone on a rectangular stand, with no on/off switch. Both products come in Sun colors and with Sun logo.

So, the new, "improved" model has no "on/off" switch, although the old one did. Maybe the new microphone is "uni-directional", but that doesn't mean it can't pick up ambient sound--just turn up the gain.

This "improvement" makes it all the more difficult to follow the final recommendation of CERT Advisory CA-93:15 (21 October 1993), quoted in

part below. It's bad enough that the problem existed in the first place, but Sun has now made it worse!

III. /dev/audio Vulnerability

This vulnerability affects all Sun systems with microphones. ...

A. Description

/dev/audio is set to a default mode of 666. There is also no indication to the user of the system that the microphone is on.

B. Impact

Any user with access to the system can eavesdrop on conversations held in the vicinity of the microphone.

C. Solution

[...]

*** Any site seriously concerned about the security risks associated with the microphone should either switch off the microphone, or unplug the microphone to prevent unauthorized listening. ***

Even if this vulnerability is fixed from a systems viewpoint, a user is still vulnerable to Trojan horse programs that exploit the user's own (legitimate) access to the microphone--and the information discussed in a person's office may be far more sensitive than the information stored on an office computer.

This is especially a problem for multi-level secure (MLS) systems. Although MLS systems offer protection against disclosure of information by Trojan horse programs, that's no help at all if the microphone picks up a Top Secret conversation that occurs in the office while the user happens to be logged in at Unclassified. Sure--one might look around to be sure there's nobody who can inadvertently overhear, or close the office door--but the computer? Computers don't eavesdrop, do they?

Computer manufacturers need to address these risks. It's certainly nifty to have desktop audio- and video-conferencing, but not when that equivalent to installing a bug in every office (and remember not to aim your video camera at the whiteboard).

Every microphone and video camera should have a positive on/off switch and some positive indication (such as a light) to show when it's actually in use (as opposed to just being enabled by the on/off switch). The broadcast industry learned this years ago, with its "ON THE AIR" lights. Fail-safes, such as permitting only manual activation, but computer deactivation, or requiring manual confirmation of any attempted activation, would be better still.

Olin Sibert | Internet: Sibert@Oxford.COM Oxford Systems, Inc. | UUCP: uunet!oxford!sibert

✓ Electronic Mail vs Paper Mail (RISKS DIGEST 15.53)

Snakes of Medusa <mathew@mantis.co.uk> Tue, 15 Feb 94 13:54 GMT

I'd just like to disagree briefly with one of the comments made in <u>RISKS 15.53</u> by Jack B. Rochester <0002757498@mcimail.com>, talking about electronic mail.

He writes that "Good grammar and proper punctuation are not required in e-mail, and their absence does not seem to affect regard for that person." I must disagree with that assertion strongly.

One particular case springs to mind, where I first met someone over the net. I got the impression that he was, shall we say, 'intellectually challenged'. When I eventually met him in real life, I was astounded to discover that he was quite eloquent. I had built up a very strong disregard for him, based on his appalling grammar, spelling and punctuation.

That may seem unfair, but people discriminate the same way in real life, as any stutterer or stammerer will know. At the risk of being contentious, my perception is that those who claim spelling, punctuation and grammar are unimportant, generally turn out to be people who cannot spell, punctuate or string together a sentence.

It's true that e-mail lacks the boilerplate formalisms of paper mail. In fact, when I get e-mail which starts "Dear Sir", it seems very odd to me. Whether the lack of generally meaningless stock phrases is a risk, I don't know. Doubtless such formalisms originally served some purpose, or else they wouldn't be there; I'm not sure that all etiquette is worth keeping in the transition from paper to screen, though. Some of it may be obsolete.

Regarding notoriety, I do still find it bemusing to discover that "real people" (from TV, films and so on) have e-mail addresses. Sometimes the lack of distance and formalism one gets with e-mail can give a whole new perspective on a person. For example, I gave in to temptation and sent electronic mail to Billy Idol. He turned out to be a really nice guy, and articulate too -- absolutely not what I was expecting from a world-famous rock musician.

mathew

★ FIRP report comments -- forward to your lists if you wish

Stephen D Crocker <crocker@tis.com> Tue, 15 Feb 94 17:12:30 -0500

Response to the Draft Report of the Federal Internetworking Requirements Panel (FIRP), 14 January 1994

Part 1: Strategic Comments

Stephen D. Crocker
Vice President, Trusted Information Systems, Inc.
IETF Security Area Director

15 February 1994

INTRODUCTION

"The Federal Internetworking Requirements Panel (FIRP) was established by the National Institute of Standards and Technology (NIST) to reassess federal requirements for open systems networks and to recommend policy on the [U.S.] Government's use of networking standards." [Preface, para 1.]

The FIRP report describes the need for the U.S. Federal Government to embrace not only the OSI protocol suite but also the ubiquitous TCP/IP Protocol Suite. In fact, Internet Standards, which include the TCP/IP Protocol Suite, are in very wide use in the Government, throughout the U.S. and throughout the world. Some OSI products and systems exist, and it may be impossible to switch completely to TCP/IP-based systems. Nonetheless, the report says, it is time to acknowledge the widespread use of the Internet Standards and give formal sanction to their use in the Government.

This is indeed a welcome change, and it should help the Government take better advantage of modern data networking.

This memo is the first of two responses to the report. In this memo, some issues are raised with respect to the recommendations in the FIRP report, and suggestions are made for avoiding problems in the future.

In the other memo, comments are given with respect to specific sections of the report.

STRATEGIC COMMENTS

This panel was convened in response to a divergence between the strategy the U.S. Federal Government had been following for several years and the direction of the marketplace. As the report makes clear, the divergence had become so great that the policy no longer reflected attainable objectives. The accommodation of the Internet Standards brings policy into line with widespread practice and removes obstacles for rational management decisions in the future.

In this light, it's worth examining the recommendations to ascertain if they are sufficient to avoid similar problems in the future. As with any large organization, the U.S. Federal Government pursues multiple policy objectives and has ingrained organizational imperatives. Recommendations that respond only to the current marketplace without also anticipating the future or without including the flexibility to follow the lead of the marketplace may lead to the convening of a similar panel in the not too distant future.

The FIRP report makes five recommendations:

1. The role of oversight and integration across federal agency internetworking activities should be strengthened within the Office of

Management and Budget.

- The roles and responsibilities for fostering standards and assessing technological change should be refocused and strengthened by the Department of Commerce.
- 3. The roles and responsibilities for infrastructure development and operations to support all internetworking services from advanced research and development to leading edge to core/commodity services should be clearly defined and formally assigned through the Information Infrastructure Task Force.
- 4. The roles and responsibilities of affinity groups should be defined, including how they are created and coordinated by the Government Information Technology Services working group.
- 5. In accordance with OMB Circular A-119, Revised October 1992, voluntary standards should be adopted and used by Federal agencies, and international standards should be considered in the interests of promoting trade. The current GOSIP policy should be modified by the Department of Commerce to reflect the wider range of international voluntary standards for internetworking.

Recommendation 1 asks that OMB's role be strengthened. OMB has the charter to review the roles, responsibilities and performances of the various agencies which provide, develop or guide the U.S. Government's internetworking activities.

This is an important role. The OMB should develop guidelines for measuring the performance of the assigned agencies and the attainment of the overall objectives. Although there is usually a preference to avoid duplication of activities, some degree of competition, exploration of alternative strategies and comparison of results is desirable because it tends to produce more cost effective products and services that are better matched to the needs of the users. Wherever feasible, the OMB should also foster multiple approaches and/or participation by multiple agencies in order to provide for maximum feedback within the system.

Recommendation 2 suggests the Department of Commerce be tasked with new responsibility for "fostering standards."

Presumably the context of this recommendation is with respect to internal standards within the U.S. Government. The general arena for developing Internet Standards is the Internet Engineering Task Force (IETF) which operates in conjunction with the Internet Architecture Board (IAB) under the auspices of the Internet Society. The Internet Society, along with NSF, ARPA, DOE and NASA, provide considerable financial support to the standards activities. This process enjoys wide spread support form the industrial, academic and government communities, and as a result, the standards developed in this arena reflect the needs of marketplace and are usually adopted widely and quickly.

Even if this recommendation is understood to be limited to refer to internal use of the U.S. Government, the recommendation is flawed. "Department of Commerce" here certainly includes NIST, but is likely to include other parts of the Department. While NIST is indeed the federal agency tasked with promoting and developing standards, NIST and the rest of the Department have at least two difficulties to overcome.

First, NIST has been the lead agency with respect to GOSIP. NIST personnel are deeply knowledgeable about the OSI suite and less familiar with the TCP/IP Protocol Suite. NIST is not now in a position to provide leadership in this area, although it does have the technical strength to follow, assist and participate in the ongoing standards activities. One challenge for NIST in the next few years will be to strengthen its staff and adjust its direction to move toward a stronger involvement in the Internet Standards activities. A significant part of this challenge is working in a standards arena in which the U.S. Government does not have de jure authority or veto power.

Second, the Department of Commerce is heavily committed to a particular strategy with respect to cryptography that is currently in conflict with the forces in the marketplace. NIST is the lead agency involved in the promulgation of the Digital Signature Standard (DSS) and the "Clipper" escrowed-key encryption system. Both of these initiatives are meeting very strong resistance from industry and academia. The RSA algorithm is the de facto standard for signatures and key exchange, and some form of DES and/or some proprietary algorithms, e.g. RC2 and RC4, are likely to be the de facto standards for bulk encryption.

The U.S. Government's orientation toward cryptography comes from the specific concerns of the intelligence and law enforcement agencies. While not denying the principle that the intelligence and law enforcement agencies have legitimate concerns, it is far from clear that the approach being taken by the Department in support of these concerns will be successful. In fact, it is entirely possible these initiatives will not succeed in the marketplace. If so, the result will be the existence of dual standards in which the Government algorithms will be used only under duress, both the Government and the general population will bear unnecessary costs dealing with dual standards, the introduction of strong security controls will be retarded, and the intelligence and law enforcement agencies will not succeed in preventing the use of strong encryption, except in so far as they succeed in retarding the use of encryption altogether. On February 4, 1994, the Department announced it had made substantial progress in its review of policies governing cryptography. Its announced that export controls on DES and similar cryptography will remain in place, that the Department will continue to promulgate the Digital Signature Standard despite uncertainties about the patent and licenses, and it will adopt the escrowed encryption system (Clipper) as a Government standard. Nothing in the public record supports these decisions, and it was made clear that these decisions are driven by the views of the law enforcement and intelligence agencies.

The purpose of citing these controversies concerning cryptography policy here is to explicate a consequence relevant to the FIRP report. The Commerce Department, and in particular NIST, have a conflict of interest. Like a lawyer with two clients with intertangled interests, the Department is trying

to serve two constituencies. One constituency is the federal government as a whole, and in that role, it must do the best job it can of interpreting the market forces and adopting federal standards that are consistent with the marketplace.

The Department's other constituency is the particular needs of the law enforcement and intelligence agencies. Those agencies desire to influence and change the direction of the marketplace. In service of this role, NIST is adopting federal standards that reflect the direction the law enforcement and intelligence agencies want the market to go.

The only way for the Department to be successful is if the law enforcement and intelligence agencies prevail and the marketplace adopts the standards the Government is promulgating. Perhaps this will happen, and if so, the Government's gamble will pay off. However, if the marketplace continues to adopt RSA as the preferred public key algorithm, if DES and other non-escrowed algorithms are used for symmetric key encryption, and if products with encryption are become prevalent in non-U.S. markets, not only will the stated goals of the law enforcement and intelligence communities be lost, the rest of the federal government and indeed the rest of the country will have paid the price in struggling with dual standards.

Like a stubborn child with a tensed jaw, the U.S. Government seems bent on pressing forward with these initiatives. So be it. But in handing out accolades because NIST is now willing to accommodate the protocols that have been commonplace for many years, it's fair to note that NIST and the rest of the Department are engaged in an exercise which promises to bring a repeat of the same divergence, confusion and waste of resources which the FIRP report documents.

Recommendation 3 suggests that each role and responsibility should be tasked to some specific agency. Apparently this is aimed at reducing duplication. While useful in principle, this approach is fragile. If the assigned agencies are incompetent or inefficient, everyone suffers. The report does suggest that some assignments may be decentralized. Decentralization should be emphasized. Wherever possible, multiple approaches and multiple agencies should be encouraged. Competition and comparison are enormously useful forces. As noted above with respect to recommendation 1, the OMB should encourage as much decentralization as possible and should oversee the agencies establishing a means of measuring the results.

Recommendations 4 and 5 are oriented toward implementation of the first three recommendations and raise fewer strategic concerns except that recommendation 5 implicitly acknowledges that the role of the U.S. Government in the standards process shift from one of controlling the process to one of participating in the process. As noted above with respect to recommendation 2, this shift poses an institutional challenge for the Government in general and NIST in particular.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 56

Thursday 17 February 1994

Contents

Smart Cards for London Buses

Mich Kabay

NII Testimony

Robert Ellis Smith

Losing ATM transactions

N.S. Youngman

Telephone charges fail to fit the bill

Marcus Marr

Re: E-mail risks

Bill Fitler

Rex Black

737 crash near Panama

Tim Steele

Re: YAMIC [Yet Another Mistaken Identity Case]

Jim Cook

Who says the Clipper issue is complicated?

D.J. Bernstein

Re: Classified justifications; escrowed keys

Carl Ellison

CFP, First Smart-Card Research & Advanced Application Conference **JJVandewalle**

Info on RISKS (comp.risks)

Smart Cards for London Buses

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 16 Feb 94 22:41:04 EST

Electronic card system launched on London's buses

--United Press newswire 02/15 1027 via Executive News Service (GO ENS) on CompuServe.

LONDON (UPI) -- London Transport Minister Steven Norris Tuesday launched

an 18-month trial of an electronic ticketing system on the city's buses. More than 200 buses operating in the Harrow district of northwest London have been fitted with a contactless "Smartcard" reader that validates bus tickets. Government officials said the trial will be the largest of its type in the world.

The article states that the credit-sized card will be activated by proximity sensors without requiring any physical contact with the reader. The card is expected to make boarding the buses easier and faster as well as reducing fraud.

Perhaps the most significant sentence in the article is the following:

"... the card will help reduce fraud and give bus operators more information about who is using their services."

I wonder if the system includes audit trails which record details of who rode which bus when. If so, I hope the software development team uses adequate quality assurance. RISKS readers will recall that Ross Anderson recently described a case in the U.K. in which a policeman was convicted of fraud for having the temerity to complain about what he claimed were unauthorized withdrawals from his bank account. The court ruled that the bank's electronic records, which _failed to support_ the defendant's arguments, were sufficient to convict the suspect.

Any system which records information about personal movements poses risks when the information is accurate; but inaccurate information can cause even more trouble.

Can a RISKS reader in the U.K. follow up on this story?

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

✓ NII Testimony

Robert Ellis Smith <0005101719@mcimail.com> Thu, 17 Feb 94 09:28 EST

PRINCIPLES OF PRIVACY
FOR THE NATIONAL INFORMATION INFRASTRUCTURE

Robert Ellis Smith
Publisher, PRIVACY JOURNAL, and Attorney at Law

Before the NII Task Force Working Group on Privacy January 26, 1994

1. Any analysis of the National Information Infrastructure must recognize that privacy includes more than an expectation of confidentiality. The right to privacy also includes (1) freedom from manipulation by others and (2) the opportunity to find safe havens from the crassness and

commercialism of daily life.

- 2. The infrastructure must be an INFORMATION-TRANSFER medium, not a SALES medium. It must be primarily an INFORMATION medium, and only secondarily an ENTERTAINMENT medium. (Will the information superhighway be only another way to exploit couch potatoes?)
- 3. It must have different levels of security and confidentiality so that some sector in it allows for confidential communications. These communications could be intercepted by law enforcement only under current Fourth Amendment guidelines. Aside from that, in the confidential portion of the infrastructure, there must be strict penalties for the interception of any PERSONAL data without the consent of BOTH the sending party and the person who is the subject of the data. And for aggrieved individuals and organizations there should be a right to sue for breaches of confidentiality.
- 4. There must be some portion of the infrastructure free from commercial messages and free from the commercial uses of the names and electronic mail addresses of the users. Even though it is commercial-free, this sector need not necessarily be operated by the government or a non-profit entity.
- 5. In the sectors of the infrastructure available for use by individuals, there must remain opportunities for ACCESSING (non-personal) data anonymously (as exist in a library situation now). Whether to permit anonymous MESSAGE-SENDING in these sectors remains, for me, an open question. To deny this will deprive the network of much of its spontaneity, creativity, and usefulness; however, to permit anonymous message-sending runs the risk of having these sectors dominated by obscene, inaccurate, slanderous, racially and sexually-insulting chatter and worse.
- 6. Privacy interests are less compelling, to me, in two other sectors of the proposed infrastructure. In those sectors transmitting proprietary business information and sensitive business dealings, the organizations using the network will see to it themselves that security meets there needs, and they will have the resources to pay for it. By the same token, in those sectors providing point-of-sale services (presumably from the home), companies offering these services will provide adequate security or risk losing customers.
- 7. The infrastructure ought not become a means for large conglomerates to transfer personal information between and among subsidiaries where the data-handling is regulated (credit bureaus, cable companies, medical providers) and

entities where the data-handling is not regulated (telephone providers, brokerages, credit-card processors, telemarketing).

Rather than proposing specific safeguards -- which can be drafted later -- the task force can be most effective in 1994 by establishing the DOMINANT THEMES of the infrastructure: information-transfer, not commercialism; democratic access not corporate dominance; diversity (in usage as well as in levels of security) not conformity.

Losing ATM transactions

<N.S.Youngman@exeter.ac.uk> Wed, 16 Feb 94 13:34:28 GMT

Recently I moved my bank account to Telephone bank PLC (names changed to protect the guilty :-), a subsidiary of Traditional bank PLC. Amongst the apparent advantages of this arrangement is the ability to use Traditional bank's ATMs.

I had a substantial amount in my current account after the transfer, much of which had come from a savings account, which gave substantially more interest than the current account does. naturally when the ATM offered me a transfer between accounts as one of its functions I elected to transfer this cash to my savings account with Telephone bank.

Nearly two weeks later I checked the balance and find that nothing had been transferred. Telephoning the bank the operator said "It doesn't allow you to do that". I offered the opinion that the ATM shouldn't offer functions it can't provide. The operator said that it couldn't be changed "otherwise the machine wouldn't recognise your card." She did however agree to look into whether there were any warnings in the banks literature (I read everything in their welcome pack and i did not see any).

The risks are obvious, but as I hate people leaving it at that, I will enumerate those that are obvious to me.

- 1 Loss of interest.
- 2 My balance isn't what I thought it was (they wouldn't reall bounce my cheques would they 8-)
- 3 Can I trust the other facilities provided by the ATM (ordering statements, cheque books, etc.)

nsyoungm@cen.ex.ac.uk youngman@signal.dra.hmg.gb

Telephone charges fail to fit the bill

Marcus Marr <marr@dcs.ed.ac.uk>

Thu, 17 Feb 94 16:21:34 GMT

The latest issue of New Scientist includes an article on the overcharging of some BT customers. The full article gives more details on the scope of the BT investigations, the perceived extent of the problem, and the steps that have been taken to notify business customers. I've tried, though, to extract the paragraphs which may be of interest to RISKS readers. There only risk I can think of is that of trusting computers, so those who cheque their phone bill should not be at risk. In my opinion, there is no risk to domestic customers since a jump of \pounds 420 in a quarterly phone bill should be noticed by the monitoring system, and if it isn't, then surely the customer would notice!

Reproduced (without permission) from New Scientist, 19th February 1994, page 18:

"British Telecom has been overcharging some of its customers because its computers cannot subtract one number from another reliably.

•••

BT is conducting two investigations, one to find out why the computer-generated bills were wrong by such a large amount, and the other to discover why the errors were not spotted by a separate computer system designed to trap gross billing errors.

BT charges calls by units (4.2 pence plus VAT). Meters at the local exchanges that log the units used on each line are read each quarter. BT's billing computer subtracts the figure for the last reading from the current reading to give the number of units it charges for.

...

In each case [of overcharging discovered], simple subtraction of the two meter readings gave a result which was wrong by 10,000 units. In one bill, four separate mistakes were discovered:

```
18497 - 2964 = 25533
14295 - 2096 = 22199
11030 - 1824 = 19206
3 - 1 = 10002
```

These four mistakes added \pounds 1680 to a bill of \pounds 3908.

BT's backup system is designed to monitor the billing computer and register any unprecedented peaks of activity on a line. But the system failed to notice any errors later spotted by subscribers.

...

Insiders say that modern digital exchanges use solid-state metering which feeds data directly into BT's billing computer. They believe that BT has a bug in its accounting software and that the problem is thus much more widespread than has so far been recognised."

★ Re: E-mail risks: appalling grammar/notoriety (mathew, RISKS-15.55)

```
<bfitler@ccmail.com>
Wed, 16 Feb 94 16:51:53 pst
```

Mathew has identified the risk of poor grammar and spelling in e-mail

messages, namely that the originator of a message will be judged as much (or more) by its form as by its content. I firmly believe that etiquette has evolved in social interactions to manage the risks of those interactions - and that the e-mail media is still young enough to be defining "proper" etiquette.

As to Mathew's comments on notoriety, several stories come to mind. Recent RISKS articles describe the flood of e-mail to Bill Gates mailbox, as well as to WHITEHOUSE.GOV. An older story describes the e-mail trials and tribulations of DEC's Ken Olsen, whose mailbox was deluged with mail, some from people who would never dare to talk to him in the hall but felt perfectly at ease taking him to task in an e-mail message.

I would greatly appreciate any pointers from RISKS readers to more information on the developing etiquette of e-mail.

-Bill Fitler bfitler@ccmail.com

Re: E-mail risks: appalling grammar/notoriety (mathew, RISKS-15.55)

Rex Black <rex@iquery.iqsc.com> Wed, 16 Feb 94 09:24:34 CST

I agree with Mathew, FWIW. As a manager, I insist on the use of proper English by all the Software Quality Assurance folks that I supervise. Why? Because, in the minds of many, as Mathew noted, hearing or reading improper English reflects poorly on the education and intellect of the person communicating. In addition, I feel that sloppy communication is a symptom of a larger problem of carelessness and lack of attention to detail, something I find inappropriate in a professional setting. How one chooses to express one's ideas is indicative of the value one places on them. Interestingly, I have worked with a number of people for whom English was a second language, and they put more effort into doing it properly--often with better results--than many who grew up speaking and writing it.

Rex

737 crash near Panama

Tim Steele <tjfs@tadtec.co.uk> Thu, 17 Feb 1994 18:38:14 +0000

This is NOT a definitive account, just my hazy recollections from having watched a "Horizon" documentary shown on the BBC this week.

Apparently, a 737 crashed near Panama about two years ago; all on board (about 47) were killed. The fault was identified by the investigating team as a probable loose wire from the gyros to the flight deck which caused the artificial horizons to "stick" in one position from time to time without any indication to the pilots that there was a fault.

The aircraft was flying at night during a storm, and the investigators thought

that a 1G roll would be undetectable to the crew; therefore, they surmised, they had no way of knowing the plane's true attitude. The resulting wild maneuvers as the pilots tried to make the stuck artificial horizons show a level attitude led directly to break-up from aerodynamic forces at about 10,000 feet.

The switches which control the artificial horizon displays were found to be set to "BOTH ON VG1" which denied the pilots information from the backup gyros. The reason for this was unknown.

The cockpit voice recorder was recovered, but proved to contain only a recording of an earlier flight; it used magnetic tape (as opposed to wire) and the tape had snapped some weeks previously. As the recorder was sealed, the tape doesn't get checked. The flight data recorder (also tape based) worked properly.

The programme implied that the team could not in the end identify the faulty wire, and had made no recommendations on modifications or checks on other 737 aircraft to prevent a reoccurrence, although they felt improved crew training might be beneficial.

Can someone post more information on this? Tim

★ Re: YAMIC [Yet Another Mistaken Identity Case]

Jim Cook <jcook@epoch.com> Wed, 16 Feb 1994 10:35:05 +0500

The indicated article stated that in month that the victim was held, his van and its contents were sold.

It would seem a second lawsuit would be indicated here for improper procedure violations. I would think that while his assets could be seized, they couldn't be sold except after conviction or a motion for a court order at which time the defendant would allowed to object.

C. James Cook, Epoch Systems, Inc., 8 Technology Drive, Westboro, MA 01581 508-836-4711x385 JCook@Epoch.com

✓ Who says the Clipper issue is complicated?

"D. J. Bernstein" <djb@silverton.berkeley.edu> Tue, 15 Feb 1994 01:13:48 -0800

"I would like to caution people about signing the petition," Dorothy Denning said. "The issues are extremely complex and difficult."%1

Clipper (by which I mean EES/Skipjack/Clipper/Capstone collectively) does raise some mildly tricky issues, which I'll discuss later. But those are _side_ issues. The basic argument%2 against Clipper is simple and deserves emphasis.

Clipper is bad because it is unfair competition in the crypto market.

Who has paid for the design and implementation of Clipper over the past decade?%3 The taxpayers. Who has paid for ramping up Clipper production at Mykotronx? The taxpayers. Who pays for the lawyers and accountants keeping Clipper on course, and the NSA-FBI team which visits Bell Labs and other locations to promote Clipper? The taxpayers. Who will pay for the key escrow ``service,'' probably an agency with dozens of people, including armed guards? The taxpayers.

I resent being forced to pay for Clipper's development and adoption.

Is this Clipper subsidy the only way that the government is interfering in the market? Not at all. Consider, for example, export controls. A private company, even if it doesn't see a foreign market for its encryption products, has to register as an arms dealer and take precautions to avoid selling crypto to non-citizens. These restrictions have been dramatically reduced for Clipper.%4

Are these points a matter of dispute? Is this just my view? No. The government knows full well that Clipper is unfair competition.

In fact, unfair competition is the goal of Clipper policy. According to Jerry Berman, "the reason [for various Clipper-related actions] was stated bluntly at the [4 Feb 94 White House] briefing: to frustrate competition with Clipper by other powerful encryption schemes by making them difficult to market, and to "prevent" strong encryption from leaving the country..."%5

Now, here's the problem: The government talks about Clipper's market interference as a good thing.

Of course, I see it as a bad thing. America's need for data protection would be fully served by a healthy encryption industry; let's eliminate crypto export controls! If you agree with me---if you want a free crypto market---then you should oppose Clipper. There's nothing complicated about this.

Let me close by briefly addressing a few side issues, mostly reasons that Clipper is risky when compared to other crypto available today.

- 1. There is a RISK that the Skipjack algorithm is, intentionally or unintentionally, weak. Suppose that in 1986 an NSA cryptanalyst noticed a subtle but wide hole in Skipjack, which was relatively new at the time. Why would it be in NSA's interest to divulge this information? Denning points out that we don't _know_ of any holes, but that's axiomatic---Clipper would be dead otherwise. One cannot deny the _risk_, exacerbated by secrecy, of a hole.
- 2. There is a RISK that Clipper will be easier to break than the basic Skipjack algorithm. Given two encryption algorithms one can (carefully) compose them to produce a ``double encryption'' which is strong even if one of the algorithms is weak. Clipper also has two encryption steps,

but for a different reason---one encryption is transparent to the user, the other transparent to the FBI. If either of these different%6 steps is weak then Clipper is weak. "Half encryption," I'd say.

- 3. There is a RISK that key escrow security will be compromised, either by bribes from the outside or by corruption from the top. It is highly dangerous to keep so many keys under the control of such a small group of people.
- 4. There is a RISK that, if Clipper fails to dominate the market, the government will simply outlaw all non-escrowed encryption. `This is a fundamental policy question which will be considered during the broad policy review.''%7 Alternatively the government could outlaw Clipper superencryption while requiring Clipper in government procurements, new phones, and so on. Denning points out that Clipper is voluntary right now, but the mere fact that the government brought up the possibility of a Clipper law means that there's a risk.

Footnotes:

%1 To sign the CPSR Clipper petition, send a message to the address clipper.petition@cpsr.org with "I oppose Clipper" in the subject header. %2 This argument was mentioned briefly by Geoff Kuenning, RISKS-15.50, among a cast of thousands.

%3 See Matt Blaze's message in <u>RISKS-15.48</u>. ``They said ... that Skipjack began development "~about 10 years ago.~"''

%4 See ftp.eff.org:pub/EFF/Policy/Crypto/harris_export.statement:

"After initial review, key-escrow encryption products may now be exported to most end users. Additionally, key-escrow products will qualify for special licensing arrangements."

%5 See ftp.eff.org:pub/EFF/Policy/Crypto/wh_crypto.eff.

%6 See Roy M. Silvernail's message in RISKS-15.52.

%7 See the initial White House Clipper press release, 930416.

---Dan

★ Re: Classified justifications; escrowed keys (Denning, RISKS-15.52)

Carl Ellison <cme@sw.stratus.com> Wed, 16 Feb 1994 14:31:19 -0500

In RISKS 15.52, Prof. Denning states (in reply to someone else):
>Certain information relating to foreign intelligence operations is
>classified. Are you saying that decisions should not be based on
>classified information or that foreign intelligence information should
>not be classified?

I am saying that decisions about the encryption I use, as a private American citizen, must not be based on classified information. I am saying that the decision must be based on a totally public debate in which we all engage. There should be no executive session, giving classified agencies an advantage over the citizenry.

She goes one to state:

>You need a court order to intercept any electronic communications, including >those on high speed nets. You need a court order to get keys. Although the >court order is not given to the escrow agents (to protect the identity of >those under investigation), certification that one was obtained must be >presented to the escrow agents.

This "protection of the identity of those under investigation" could actually be protection of agents doing illegal wiretaps. If the escrow agents were to give not the master key for a chip but a session key and if each request for a session key included the name of the person being tapped and the court order authorizing it, then the escrow agents would be in a position to notice the kind of abuses for which Nixon and Hoover were famous and therefore would be able to blow the whistle on the offending agency.

✓ CFP, FIRST SMART CARD RESEARCH AND ADVANCED APPLICATION CONFERENCE

Jean-Jacques Vandewalle <jeanjac@iad.ift.ulaval.ca> Tue, 15 Feb 1994 22:45:52 GMT

CALL FOR PAPERS: CARDIS
FIRST SMART CARD RESEARCH AND ADVANCED APPLICATION CONFERENCE
October 24 - 26, 1994 LILLE FRANCE
Sponsored by IFIP - The International Federation for Information Processing

AIMS AND GOALS

Smart cards or IC cards are becoming a significant part of the information processing world. Furthermore they are beginning to move towards real integration into the information systems. They participate in the overall data management, security and communication processes. But they bring their own special characteristics. It is very likely that future IC cards will require many scientific and technical improvements which represent a challenge for the success of the technology. So far there are many events which are mostly devoted to the commercial and application aspects of IC cards. There is now an opportunity to initiate a scientific conference bringing specialists who are involved in all aspects of design of the future IC cards and related devices and environment. IFIP - the International Federation for Information Processing has agreed to sponsor this conference. It will be the first occasion for the IC card community to start a permanent activity: In addition to the conference itself there will be discussions about creating a permanent group within IFIP with possible implication for advancing standards, publishing and international cooperation.

SUBMISSIONS

Six copies of detailed abstracts of original papers corresponding to one or several themes for the conference should be sent in English to the program chairman before May 2, 1994. The submissions will start with a succinct statement of the problem addressed and their significance, appropriate for a non-specialist. Technical development directed to the specialist should follow as needed (at most ten pages).

They should be accompanied by a fact sheet indicating the following:

- Title of the paper with the relevant conference theme(s);
- Author(s) with affiliation, address, phone and fax numbers, E-mail.

Proceedings will be available at the conference.

IMPORTANT DATES

Submission deadline May 2, 1994
Acceptance notification June 17, 1994
Camera ready paper due August 13, 1994
Conference October 24 - 26, 1994

THEMES

TECHNOLOGY

IC architecture and techniques

Memories and processor design

Read/Write unit engineering

Specific co-processors for cryptography

Biometry

Communication technologies

Interfaces with the owner, the service suppliers

Reliability and fault tolerance

Special devices

Standards

SOFTWARE

The operating system

Models of data management

Communication protocols

IC CARD DESIGN

IC cards formal specification and validation

Tools for internal or external software production

Validation and verification

Methodology for application design

SECURITY

Models and schemes of security

Algorithms

Security interfaces

Hardware and software implementation

Security of information systems including cards

Formal verification of transaction sets

IC CARDS, INDIVIDUALS AND THE SOCIETY

IC cards and privacy

Access to his data by the owner

IC cards: political and economical aspects

Is the IC card going to change regulation?

Patents, copyrights

FUTURE OF THE IC CARDS

Innovative technologies

Moving towards the pocket intelligence

Convergence with portable PCs, laptops etc ...

PCMCIA

INNOVATIVE APPLICATIONS

Design methodology of applications IC cards and the information system Examples of new applications
Requirements for innovative cards

ORGANIZATION

General Chairman Program Chairman

Prof. Vincent Cordonnier Prof. Jean-Jacques Quisquater
RD2P Universit'e Catholique de Louvain
CHRU CALMETTE Dept. of Electrical Eng. (DICE)

Rue du Prof. J. Leclerc Place du Levant, 3

F - 59037 LILLE CEDEX B - 1348 Louvain-la-Neuve

FRANCE BELGIUM

Tel (33) 20 44 60 47 Tel (32) 10 47 25 41
Fax (33) 20 44 60 45 Fax (32) 10 47 86 67
e-mail: cardis@rd2p.lifl.fr Quisquater@dice.ucl.ac.be

Program committee

Mart'in Abadi (Dec Research, USA)

Ross Anderson (Cambridge, UK)

Benjamin Arazi (Ben-Gurion, Israel)

Todd Arnold (IBM, USA)

Jacques Berleur (FNDP, Belgium)

William Caelli (Queensland, Australia)

David Chaum (DigiCash, Netherlands)

Vincent Cordonnier (Lille, France)

Mark Cummings (SRI, USA)

Amos Fiat (Tel-Aviv, Israel)

Andr'e Gamache (Quebec, Canada)

Marc Girault (SEPT, France)

Louis Guillou (CCETT, France)

Joseph Hoppe (TRT Philips, France)

John Kennedy (Cylink, USA)

Philippe Maes (Gemplus, France)

Roger Needham (Cambridge, UK)

Jean-Jacques Quisquater (Louvain-la-Neuve, Belgium)

Laurent Sourgen (SGS-Thomson, France)

Doug Tygar (Carnegie-Mellon, USA)

Michel Ugon (Bull-CP8, France)

Klaus Vedder (GAO, Germany)

Robert Warnar (NIST, USA)

The city of LILLE is about 150 miles away from PARIS. It can be reached: from Paris by either motorway (two hours) or train (one hour). From most European countries by train, motorway or plane. The conference will take place at the University of Sciences and Technology of Lille. Accommodation can be provided either on the campus or in the center of the Lille. We will provide maps and help for hotel reservation and travels.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 57

Tuesday 22 February 1994

Contents

- Extra line in Chemical Bank program doubles ATM withdrawals John Sullivan
- What else happens when the airbag in your car is detonated? William Caloccia
- SimHealth
 - Mike Zehr
- Risks of "doing it right"
 - **David Wittenberg**
- The ultimate couch potato
 - **Bruce Balden**
- Telephone Card Audit Trails
 - F.Baube[tm]
- E-Mail Courtesy
 - **Dan Yurman**
 - Peter Cherna
 - Greg J B
- E-mail to Bill
 - **Aaron Barnhart**
- CompuServe Offers Credit Info
 - John Murray
- Electronic Food Stamps
 - LoQuan Seh
- Re: YAMIC [Yet Another Mistaken Identity Case]
 - **Bryan J Dawson**
- John Perry Barlow WiReD article on Clipper
 - **Martin Minow**
- Info on RISKS (comp.risks)

Extra line in Chemical Bank program doubles ATM withdrawals

John Sullivan <sullivan@msri.org> Sat, 19 Feb 94 19:55:58 PST

An extra line meant to be "dormant" for now caused Chemical Bank to deduct

twice any amount its customers withdrew from ATM machines Tuesday night and Wednesday. However, they received praise from the state consumer board for their prompt and open response to the problem.

My information comes from articles in The New York Times, 18 Feb 1994, p. A1 and 19 Feb 1994, p. C1. The new line of code was part of a year-long effort to add functionality to ATM machines. It sent a copy of the ATM withdrawal to a different computer system (the one that handles paper checks), which then deducted the money a second time. This second system is only run overnight, so the problem was not detected until Thursday morning.

About 430 checks were bounced incorrectly as a result, but Chemical contacted the customers affected, and offered to pay any charges they incur, or write letters of explanation to the recipients of the checks. The NY state consumer board has also asked them to refund any fees for the ATM transactions which were completed incorrectly.

There were about 150k ATM transactions incorrectly doubled, amounting to \$15M. (Last year in the US there were 7G ATM transactions averaging \$50, according to The NYT article.)

Steven Bloom, who runs a consulting firm in NJ said: "There are similar episodes that take place all the time, but we never hear about them because the bank is able to get the accounts straight before it opens its doors in the morning. The problem in this case is the ATM system is highly visible and runs 24 hours a day, seven days a week."

-John Sullivan@geom.umn.edu

[Also noted by
Linn H. Stanton <stanton@acm.org>,
Mark Bergman <bergman@panix.com>,
Jeremy Epstein <jepstein@cordant.com>,
"Greg D." <greg@io.org>, and PGN.
I took John's version because his version was the
most Digest-able, although not entirely consistent with the others.
Further sources included the following clips:]

In one of the biggest computer errors in banking history, Chemical Bank mistakenly deducted about \$15 million from more than 100,000 customers' accounts on Tuesday night, causing panic and consternation among its customers around the New York area.

The mistake affected 150,000 transactions from Tuesday night through Wednesday afternoon. Some checks were bounced Thursday morning as a result, although the bank said the number was small.

[The New York Times, Friday 18 Feb 1994]

Millions of dollars vanished from New Yorkers' bank balances Wednesday, when a computer deducted \$2 from accounts for every \$1 withdrawn from automated teller machines." [...]

Sean Kennedy, president of the Electronic Funds Transfer Association (a trade group) said "I'm beginning to learn that it does happen from time to time [and] usually it's a software error".

[The Washington Post, 18 Feb 1994, from Jeremy Epstein]]

Customers stormed into Chemical Banking Corp's branch offices to complain of empty accounts and bounced cheques after a computer glitch affected at least 70,000 of the bank's approximately one million customers.

[The Financial Post, a Canadian business paper, from Greg D.]

What (else) happens when the airbag in your car is detonated?

William Caloccia <caloccia@sw.stratus.com> Thu, 17 Feb 94 17:25:49 -0500

[Autoweek 7 Feb. 1994]

A British Ford dealer set out to impress potential purchasers with the burglar-proof features of the new Ford Mondeo by staging a break-in in his showroom.

As a room full of potential customers watched, the hired thief walked up to the front of the car and gave it a swift kick in the bumper, near the airbag sensor. The bag inflated, AND the central locking system disengaged. The thief then opened the door, quickly broke the steering column lock, hot-wired the ignition and started the car.

News spread quickly, and copycat incidents have followed.

Autoweek says "Sales of The Club should increase."

Historical Anecdote:

Word from friends in MoTown, was that when Ford was testing the very first airbags in Police cars, the fuel cut-off relay would also be triggered by the same impact sensing circuit. Street-wise evaders found this out and they would tap the bumper to trigger the airbag if the cops were too close in pursuit, disabling the vehicle. (This also may have been how Ford was able to guarantee the ability to inspect the vehicle after the bags were deployed, as it was a testing situation.)

--Bill caloccia@Team.Net caloccia@Stratus.Com

[The first item was also noted by Chip Olson. PGN]

SimHealth

Mike Zehr <mikez@kenan.com> Wed, 16 Feb 94 14:12:22 EST

Maxis Business Simulations, the creators of SimCity, have a new product called "SimHealth." The program is a simulation of a health care system, incorporating features from the new Clinton (US) health care proposal and other plans dating back to Truman (US president from a number of years ago). The other Maxis products are sold as games, and I imagine this one is sold

that way too, but the February issue of CIO describe it as "to help the public better understand the complicated issues that underlie the nation's health-care debate." Furthermore, they attribute Maxis as "envision[ing] SimHealth being used by a wide range of concerned citizens to evaluate current policy and new proposals."

The obvious risk is a public that expects a certain policy to work because it works in SimHealth. (Admittedly it is juse a game. But in addition to the benefits simulations give, there is always the danger that too much trust will be put in a simulation, or that the beliefs of the simulation developers will be giving too much credence after being filter through a computer.)

michael j zehr sr. software engineer kenan systems corporation

✓ Risks of "doing it right"

David Wittenberg <dkw@cs.brandeis.edu> Tue, 22 Feb 1994 14:38:56 -0500 (EST)

>From "The New York Times Magazine" February 13, 1994:

"It's a thin plastic card that will completely change the way you pay fares on New York City's subway and buses. No more searching for tokens in pockets or purses. Metrocard is convenient to carry and easy to use."

So says the M.T.A. [Metropolitan Transit Authority] in its brochure on the new Metrocard, which can be obtained in several denominations and used instead of tokens in a number of subway stations. But -- and there's always a but -- should any problems arise, then, in the dim light in the wee hours at Grand Army Plaza, follow these instructions:

"... Try it again and check the turnstile display to see what it says. If the card still doesn't work, try another turnstile. If the second turnstile doesn't let you enter, see what the Metrocard Reader near the turnstile says when you swipe the card there. If the information displayed on the Reader doesn't explain the problem, ask the clerk at the Metrocard window in the token booth for assistance."

[description of what conditions the clerk can fix - often the clerk can give you a replacement immediately, when to mail the card in for a replacement, and addresses and phone numbers for assistance]

[The Times adds this comment:] Meanwhile, carry spare tokens.

Here the MTA has apparently done a good job of identifying likely problems, and providing solutions. They've explained what to do, and what they can do if something doesn't work. (I don't know the details, so I don't know if they have identified the right set of problems, but they've done a much better job than most new installations of card readers.) The language is slightly technical (In particular is "swipe" widely used?) but the directions for trouble shooting are quite clear.

What do they get for their care? A cheap shot from the Times. Had they just said "the Metrocard will work perfectly" (as many places have), RISKS readers would smirk, but the Times would probably not have commented. As we've gotten more cynical about computerized systems, we've made it harder for the organizations which do plan for problems to get credit for their forethought.

A week later (Feb. 21), the Times had an article saying that distribution of the first 40,000 cards went smoothly. Perhaps the MTA really has done a good job.

--David Wittenberg dkw@cs.brandeis.edu

The ultimate couch potato

Bruce Balden <balden@wimsey.com>
Sun, 20 Feb 1994 23:17:27 -0800 (PST)

Recently, I heard the Chairman of Sun Microsystems on California Commonwealth, a Bay-area radio program, lampooning the National Information Infrastructure (aka information superhighway), and in particular lambasting its vision of doing everything at home. In his view, this would lead to birth of the ultimate couch potato.

Those interested in the risks of computing should contemplate the following notion: is it possible to make communications too effective?

When I heard Scott McNealy give his comments, my mind went back to a story by E.M.Forster, called The Machine Stops. This story, written before WWI, imagines a world where the NII is in place but the rest of the world has gone to hell, quite literally, and everybody has degenerated into couch potatoes. This, they imagine, is paradise until the Machine stops!

Merchant and Ivory have had such a great time and made a lot of money turning other Forster stories into movies (Passage to India, Howard's End, A Room With a View). I think they should look this one over too. Should make quite a thriller.

Bruce Balden Wimsey Information Services balden@wimsey.com

Telephone Card Audit Trails

F.Baube[tm] <flb@flb.optiplan.fi> Sat, 19 Feb 94 0:50:16 EET

Here in Turku Finland one can make calls from pay phones using prepaid cards issued by the city phone company, Turun Telelaitos. These cards are on sale throughout the city, and are bought anonymously for cash.

On two different occasions I have had cards malfunction. When the card is placed in a phone it is read and seen as valid, and I can dial, but when the other party answers, and the card is locked in for debiting, an error is

generated and the call is (frustratingly!) terminated.

On both occasions I have taken the offending card to the phone company's office. The card is passed thru a reader which displays the card's unique identifying number. The service person then calls this number in to another bureau, where they can dump a complete calling history of the particular card, no doubt to verify malfunction and protect themselves against fraud.

Having verified the card malfunction, the service person asks for a name and address before issuing a refund (in the form of another card) for the malfunctioning card's unused portion. I do not know whether the name and address are ever verified; in this country I would imagine not.

It is all well and good that they can extensively track an individual card, and where it has malfunctioned, and that this card can be bought anonymously, but naturally my privacy breaks down when they take my name and address, which they can (in principle) match it to the card's audit trail to get a partial track of my calling activities.

But given that such card malfunctions are an unusual occurrence, related perhaps to the recent spate of subzero (fahrenheit) weather, it does not seem to me to be an undue threat to my privacy.

Nonetheless, can anyone suggest some ideas that I might take to the phone company to permit them to make the same checks but with a higher level of privacy? Or should I just give them a bogus name and see if it ever causes a problem (in the form of, for example, more intrusive checks before issuing refunds)?

* Fred Baube(tm), GU/MSFS/88 baube@optiplan.fi

Email Courtesy

Dan Yurman <dyurman@igc.apc.org> Fri, 18 Feb 1994 07:29:28 -0800

Bill Fitler (bfitler@ccmail.com) asks about email courtesy issues in RISK 15.56.

Perhaps one disturbing trend as more people use Internet is the practice by college students of using subject matter listservs as sources of first resort for information they should be looking up in their university library. Every year BIOSPH-L@UBVM.BITNET, a list dealing with environmental issues, is flooded with ill-expressed questions that should not be addressed to the list. These include questions such as "what is hazardous waste," etc. Another which came up today was a question which could be answered by using the Statistical Abstract of the US or any World Almanac, etc.

Last year a hot debate erupted when a graduate teaching assistant at a major, dare I say, top 10, Eastern university, assigned a class of undergraduates to use Internet to seek information on research paper topics. The TA did not instruct the students to use the library first and then pose well formulated

questions to the net. BIOSPH-L was flooded with questions on basic environmental science.

Both the TA and the students were outraged by the complaints they received from list readers who objected to being asked fundamental questions that ought to be dealt with by the students themselves. The root cause appears to be neither the TA nor the students had any idea who was at the other end of the line. All they saw was a computer that should be giving them answers.

What was said to them repeatedly is this. The courtesy issue is that traffic on BIOSPH-L is voluntary. If you want people to take the time to answer your questions, indicate you have done some legwork on your own and have a genuine problem looking for additional information. Otherwise, you are soaking up volunteer resources which could be better used to meet needs not answered elsewhere.

Also, neither the students nor the TA took kindly to suggestions that if they absolutely insisted on using computer terminals instead of (gasp) books, that there are online services which for a fee will gladly give them the information they want.

Dan Yurman dyurman@igc.apc.org Idaho Falls, ID 43N112W -7 GMT

★ Re: E-mail risks: appalling grammar/notoriety (mathew, RISKS-15.55)

<pcherna@BIX.com>
Tue, 22 Feb 1994 09:19:13 -0500 (EST)

Another RISK of the high prevalence of poor grammar and spelling in e-mail is the risk to one's own style. If immersion in a foreign language is an established way to improve one's fluency in that language, then surely immersion in a medium where capitalization, spelling, punctuation and grammar are weak might harm one's own ability to compose correctly. I've found that I sometimes question my own use of "it's" vs. "its", which I never had trouble with before I used e-mail, for example.

Peter Cherna -- pcherna@bix.com

Re: E-mail Etiquette

<gjb@fig.citib.com> Thu, 17 Feb 1994 17:45:32 -0500

In the U.S., the CBS television network airs an "Olympic Late Night" show every night at 11:30 p.m. or 12:30 a.m. The show is a sort of hip, MTV-style rundown of the day's events in Lillehammer. The show also does a nightly "Information Highway" segment, and maintains a forum and e-mail address on Prodigy. Wednesday night, for instance, host Pat O'Brien sat down at a PC and personally answered e-mail from a doting user. On the air, O'Brien tells viewers to send Prodigy e-mail to "Ask Pat O'Brien". (And he doesn't mention whether there are spaces, hyphens, or anything else in his address.)

Some readers of the rec.sport.olympics newsgroup are upset with the CBS coverage, so someone suggested mailing "obrien@prodigy.com". The poor Prodigy user with the username "obrien" was understandably upset when his mailbox flooded with harsh criticism of the CBS Olympic coverage. I don't know if other Prodigy users joined Internet users in sending their CBS-bashing to the wrong address, but poor Mr. O'Brien had to have his e-mail address changed.

greg

✓ E-mail to Bill

Aaron Barnhart <barnhart@mcs.com>
Thu, 17 Feb 94 16:19 CST

According to the 21 Feb 1994a _Business Week_, Microsoft chairman Bill Gates has never had anyone screen his electronic mail. With the recent publication of his e-mail address in _The New Yorker,_ however, he's reconsidering.

While in the short run that would be a good idea, I don't know why Gates hadn't installed aliases and mail filters long before. Now I suspect that Microsoft Mail doesn't even have these capabilities.

Aliases would allow re-routing of mail to billg, but with a different "To:" header. In combination with mail filters, Bill could give out a separate VIP address and send all non-VIP mail to a reserve mailbox for a staffer to read.

CompuServe Offers Credit Info (From AP News Service)

John Murray <jxm@engin.umich.edu> Tue, 22 Feb 1994 19:52:55 -0500

CompuServe Inc. and National Information Bureau Ltd. (NIB) have agreed to give CompuServe users access to NIB's credit information, as well as motor vehicle, workers' compensation, real-estate, tax, crime, and employment databases --- subject to "several levels of security" (which may seem like a bad joke to some RISKS readers). [PGN Abstracting Service]

Electronic Food Stamps

LoQuan Seh <eng350d3@csulb.edu> 18 Feb 1994 01:45:27 GMT

Electronic food stamps might be a good way to prevent fraud, but they also may make it easier to steal from the government. It will stop thieves from robbing the food stamp from people's mail, but thieves may be able to use computers to steal from the accounts on the card. The criminals use of technology to commit food-stamp fraud may be more educated than the criminals who were robbing mail boxes.

★ Re: YAMIC [Yet Another Mistaken Identity Case] (Cook, RISKS-15.56)

Bryan J Dawson <dawson@ornews.intel.com> 17 Feb 1994 16:43:14 -0800

I would think that while his assets could be seized, theycouldn't be sold except after conviction or a motion for a court order atwhich time the defendant would allowed to object.

Sorry, but no. His property was no doubt subject to 'Civil Seizure' (probably the single MOST SERIOUS threat to the foundation of the US constitution). Under 'Civil Seizure' a strange legal circumlocution allows the PROPERTY to be arrested because it 'participated in a crime' and since property cannot defend itself there is no due process. The only recourse for the prior owner is for him to sue for its return and HE MUST PROVE THE PROPERTY IS 'INNOCENT' (note no assumption of 'innocent until proven guilty'). Furthermore, there is a fairly short period of time during which the prior owner must take action or his property is considered 'abandoned' and he has no further recourse.

I'm not a lawyer, a legal expert, or even an expert on Civil Seizure but the above comments are substantially correct...

(C) 1994

✓ Wired article on Clipper

Martin Minow <minow@apple.com> Fri, 18 Feb 94 11:43:09 -0800

The April 94 issue on Wired will have an article on Clipper that is probably relevant to Risks readers.

WIRED 2.04 Electrosphere: Jackboots on the Infobahn

Clipper is a last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace.

By John Perry Barlow

[Note: The ... article will appear in the April 1994 issue of WIRED. We, the editors of WIRED, are net-casting it now in its pre-published form as a public service. Because of the vital and urgent nature of its message, we believe readers on the Net should hear and take action now. You are free to pass this article on electronically; in fact we urge you to replicate it throughout the net with our blessings. If you do, please keep the copyright statements and this note intact. For a complete listing of Clipper-related resources available through WIRED Online, send email to <infobot@wired.com> with the following message: "send clipper.index". - The Editors of WIRED]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 58

Weds 23 February 1994

Contents

E-Mail blunder at Olympics

David G. Novick

Dog Gets Card With \$10G Limit

marc via PGN

Computer error adds to ad valorem tax for 300,000 people

James E. Burns

Embezzler caught by computer trail

James E. Burns

Software testing at Sizewell

Brad Dolan

Clipping Clinton and the Executive Branch...

Peter Wayner

Clipper: Love your country, don't trust its government

David Honig

Re: CompuServe Offers Credit Info

Steve Bellovin

Social RISKS of Universal IDs

John Oram

Re: SimHealth

Gerd Meissner

Bob Frankston

Re: Telephone Card Audit Trails

Jonathan I. Kamens

Re: E-Mail Courtesy

Jim Haynes

Bob Frankston

Re: Electronic Food Stamps

Colby Kraybill

Re: International Internet Association

Jeff Porten

Info on RISKS (comp.risks)

✗ E-Mail blunder at Olympics

David G. Novick <novick@cse.ogi.edu> Tue, 22 Feb 94 22:08 PST

Here's another example of a familiar problem with a topical twist, as reported by the Portland "Oregonian" February 22, 1994, p. C5:

"Access Violation: Several U.S. reporters were contacted by Mike Moran, the U.S. Olympic Committee chief press attache, after they got Portland figure skater Tonya Harding's Olympic identification number and broke into her computer mail program.

"All persons with Olympic credentials have access to a computer mail system on which they can send notes to others and receive information. Access is is through an individual's Olympic ID number and a password, typically the user's birthdate.

"The reporters got Harding's ID number through a blown-up photo and typed her birthdate to gain access to her messages.

"The skater had received 61 messages by Sunday."

David G. Novick, Dept of Comp Sci & Eng, Oregon Grad. Inst. of Sci. & Techn., P.O. Box 91000, Portland, OR 97291-1000 novick@cse.ogi.edu (503) 690-1156

✓ Dog Gets Card With \$10G Limit

<marc@MIT.EDU> Wed, 23 Feb 94 00:57:23 EST

We've all read stories here of how credit agencies have make mistakes. Sometimes, it isn't the consumer who loses. Marc

[The PGN Excerpting Service provides the following summary of an AP item from Ballston NY, relayed by clarinews@clarinet.com, 14 Feb 1994. PGN]

An eight-year old Brittany spaniel has her own \$10,000 line of credit. Her owner began using her name on coupons and warranties, which then resulted in solicitations and finally an offer of a credit card. [Her pawtograph is apparently enough when she charges dog food. Perhaps she pours arf-and-arf over it.] PGN

✓ Computer error adds to ad valorem tax for 300,000 people

James E. Burns <burns@gauss.bellcore.com> Wed, 23 Feb 94 15:48:27 EST

The Atlanta Journal of 18 Feb 1994 carried an article by Chris Grimes describing an error in 300,000 auto tax bills (about 5% of the total). The error added \$10 to \$30 to the ad valorem portion of the bill. Apparently the mistake was caused by a patch added to correct a similar problem from the

previous tax season. (Once again, the rule of thumb that a change to fix a bug has a 50% chance of introducing a new one seems to hold.) Officials expect the problem to be fixed for next year's tax season. (One wonders if the have a "three strikes and you're out" rule :-)

Apparently, the State is not notifying motorists directly of the incorrect amounts --- they must contact their local tag offices to ask if there was an error. The article warns, however, that this might result in a higher bill since the errors apparently were both postive and negative.

James E. Burns, Bellcore, NVC-3X114, 331 Newman Springs Road, Red Bank, NJ 07701-5699 burns@nova.bellcore.com (908) 758-2819

Embezzler caught by computer trail

James E. Burns <burns@gauss.bellcore.com> Wed, 23 Feb 94 15:34:33 EST

An article by Davidson Taylor appeared in the 18 Feb 1994 issue of the Asbury Park Press (NJ) described the arrest a teller of a local credit union for embezzling \$15,000. The embezzling was allegedly done on the teller's last day of work, 8 Mar 90. There is a supposition that the teller might have destroyed the paper trail; she was apparently caught through computer auditing by the Federal Reserve, which notified the credit union on 19 Mar 90. No clear explanation was given for the nearly four year delay in filing charges.

Of interests to RISKS readers was the quote from Assistant U.S. Attorney Jay McMahon regarding the detection of the fraud:

"You can't destroy computer records."

James E. Burns, Bellcore, NVC-3X114, 331 Newman Springs Road, Red Bank, NJ 07701-5699 burns@nova.bellcore.com (908) 758-2819

Software testing at Sizewell [Note: British NII is not US NII]

Brad Dolan

bdolan@well.sf.ca.us>

Wed, 23 Feb 1994 12:32:02 -0800

TESTING THE SOFTWARE [Nuclear Engineering International, 12/93, p.10]

Britain's Nuclear Installations Inspectorate is satisfied that the software for the Sizewell B Primary Protection System (PPS) will be adequate for its role - provided that no further major issues arise from NII's continuing assessment or from the commissioning trials now underway, that the various ongoing independent assessments are completed successfully, and that a "clean" dynamic testing demonstration is achieved.

The NII does not believe that Nuclear Electric's original PPS integrity target (10E-04 probability of failure per demand as proposed in the Pre-Construction Safety Report) has been fully demonstrated - it was always regarded as a very

tall order by the regulators - but it does accept that the overall safety case for the plant "can accommodate, without significant detriment, a lower integrity for the PPS."

These conclusions are part of a status report on NII's assessment of the PPS presented by NII staff to the Advisory Committee on the Safety of Nuclear Installations on 1 July. In October, the UK trade newspaper _Computer Weekly_ took the innovative step of helping the nuclear industry in its mission to be more transparent by making the leaked report available to readers (at 2 pounds to cover copying and postage).

The NII notes that two main themes have emerged from its assessment of the Sizewell B PPS software. On one hand there is complexity of design, which "has made the task of demonstrating a high integrity for the system particularly difficult." On the other hand there is the compensatory effect of examination and testing, not only by the supplier, Westinghouse, but also by a range of organisations in the UK: "no other reactor protection system in the world, past or present, has received more attention than the PPS" (see NEI, March 1993, pp. 28-33, for a flavour of the 500 person-year effort).

Because of the difficulties of quantitative demonstration of software reliability, NII has adopted a "special case procedure" consisting of two legs: demonstrating excellence of production; and an onerous programme of confirmatory independent assessment, to build confidence that the required dependability has been delivered (see NEI, September 1991, pp. 38-40).

The independent assessment is still going on. Because of the huge effort entailed, it was always expected to "run right up till the eleventh hour" says David Hunns of the NII.

The dynamic testing, which has received a good deal of publicity recently, is just one part of the independent assessment programme. Originally offered by the utility on a voluntary basis, the dynamic testing uses a "test harness" to subject an actual guardline of the PPS to a sample of the inputs it might see during selected fault scenarios and then to compare the output from the guardline against what it should have been according to a logical model based on the specifications of the PPS.

Unfortunately, in about 52% of the 49694 valid tests performed in the 6 month programme ending December 1992 there was a discrepancy between the actual and expected PPS output. About 90% of the failed runs have been ascribed to inadequacies of the test harness (in particular limitations in its modelling of PPS characteristics) rather than the PPS itself, but the NII wants a complete explanation of all the reasons for failure and demonstration of a "clean" test run the test harness performing satisfactorily. More tests are underway.

Brad Dolan bdolan@well.sf.ca.us 10ATT.0.700.NUCLEAR ask me about PGP

Clipping Clinton and the Executive Branch...

Peter Wayner <pc@access.digex.net>

Wed, 23 Feb 1994 13:28:19 -0500

In a recent samizdat, I've heard that the National Intelligence Agencies are urging the White House to use Clipper for its own internal system. It sounds like a good plan to lead by example, right?

Unfortunately, I would resist using such a system if I was the President. Why? Because Washington is filled with intramural spooks watching other branches of the government. Most of the folks in privacy groups like to imagine the Clipper chip as an instrument of government oppression directed toward the common folks. In reality, I would bet that a number of phone taps are agency-vs-agency, intramural things.

For instance, Bill Safire found out that his phone was tapped while he was a speechwriter for Nixon. A recent internal investigation by the DOJ revealed that there was an internal eavesdropping system for listening into different branches of the DOJ. Internal Phone calls were routinely recorded.

This is why, I believe, that 13 state legislatures ban their state and local police from using phone taps. These taps would give the folks who run the local police a good deal of intelligence about state-wide issues and spending.

This is also why the recent Bush-to-Clinton transition was such a mess. The clintonians arrived to find computers stripped of their hard disks. Why? Because it is possible to retrieve info from hard disks long after they've been erased. Also, the Clintons stripped out the phone system and had a new one installed? Why? Who knew what bugs were left in place.

Of course the most important reason not to adopt the Clipper for White House use was on the cover of the NYT today. A CIA analyst was finally caught spying for the Soviets. He was supposed to have netted at least 1.5 million dollars for his information.

I was particularly struck by the size of the house that he bought for \$500,000 in allegedly ill-gotten cash. It wasn't that big. Life in Washington is very expensive-- especially for the clerks and career employees of NIST and the Treasury Dept. If you need to sell out to get this house, it must be tough to sit there on top of hte keys to every conversation in america and be happy in your rundown bungalow and Reagan era sedan.



Date: Wed, 23 Feb 1994 11:31:11 -0800

From: David Honig <honig@ruffles.ICS.UCI.EDU>

Subject: Clipper: Love your country, don't trust its government

[... Further comment after noting the CIA story:]

So, you can buy a high ranking CIA person (who ran the *counter*intelligence branch for 2 years) for a measly \$1.5 million. I wonder how much a pair of Clipper-key-escrow agency people will cost?

Re: CompuServe Offers Credit Info

<smb@research.att.com>
Tue, 22 Feb 94 22:49:24 EST

CompuServe Inc. and National Information Bureau Ltd. (NIB) have agreed to give CompuServe users access to NIB's credit information, as well as motor vehicle, workers' compensation, ...

The AP ran a correction to this story today. They noted that only National Information Bureau customers would have access to the information. (But the article did not say how that would be enforced.)

[Also noted by Chuck Weinstock <weinstoc@SEI.CMU.EDU>. PGN]

Social RISKS of Universal IDs

John Oram <oramy92@halcyon.com> Wed, 23 Feb 1994 01:00:23 -0800

This was in the op-ed section of the Globe & Mail last Friday (23 Feb). As it is a relatively non-technical description, I'm not sure how appropriate it is for this forum, but it presents a fairly eloquent argument outlining the potential social RISKS of universal ID cards.

=-=-=-=

Your identity card please

Ontario's Social Services Minister is worried about welfare fraud, but doesn't want to stigmatize welfare recipients by singling them out for fingerprinting. So Tony Silio has seized on a clever alternative: require _everyone_ in Canada, whether or not they are on welfare, to carry a universal identity card. Citizens wouldn't have to clutter their wallets with a separate driver's license, age-of-majority card, health card and so on. It would be adorned with a photograph and (possibly) a digitized fingerprint. How efficient. How practical. How unwise.

It's always difficult to argue against such schemes because they are, on the surface, so sensible. There is no doubt at all that a universal ID card would make life easier for all kinds of authorities, from the welfare people (who could easily prevent multiple claims) to health care administrators (who could catch out-of-province and out-of-country freeloaders) to the police (who could quickly check the identity of suspected wrong-doers, whether or not they are licensed to drive). For honest Canadians, they would make daily life a little more convenient without posing any immediate threat -- just as photo radar on the highways poses no immediate threat to people who do not speed, or video cameras on street corners pose no immediate threat to people who don't vandalize public property. Why, then, do all these things give us a chill?

Critics would say it is irrational fear, an automatic reaction to any measure, however reasonable, that reeks of Big Brother. They would be partly right.

Few opponents of identity cards really expect Canada to become a police state the day after they are introduced. Their opposition springs instead from instinct, a gut feeling that a society that makes its members carry an identity card is, however intangibly, less free. It is, on the whole, an admirable instinct.

There are many practical objections, too. The very existence of a unified identity card would invite invasions of privacy. Advances in microchips and other technologies have made it possible to put an immense store of information on a simple plastic card. If such a card can carry a digitalized fingerprint, it can also be designed to contain the holder's medical history (handy for insurance companies), credit record (convenient for banks and stores) or criminal record and probation status (nice for the police). Thanks to computer networks, this sort of information can easily be shard among various agencies.

At present, we are at least partially protected by the fact that we carry separate cards for separate things. A person who is pulled over by the police for speeding expects to hand over his driver's licence because he knows that holding such a license is required to operate a car. He does not expect simultaneously to hand over his welfare, medical or employment ID. The merit of separate cards is that each agency of the government has access only to the information that it clearly and demonstrably needs.

Canadians already must carry a host of identification cards they did not need on the past. Ontario, for example, only recently required residents to present a health card when visiting the doctor. Until 1964, there was no such thing as a social insurance number. But if a citizen is not applying for a job, paying his taxes, going to the doctor or driving a car, he can still leave his wallet and home and walk down the street without a scrap of identification in his pocket, defined not by a piece of plastic but by his status as an individual. That is a feeling that citizens of most countries do not enjoy. It is one Canadians should not let slip away.

Re: SimHealth (RISKS-15.57)

Gerd Meissner <100064.3164@CompuServe.COM> 23 Feb 94 05:19:42 EST

SimHealth, introduced in Washington D.C. last November, was developed by Maxis Business Simulations, which is a special unit of that company. It was developed, as I've learned, for the Markle Foundation as kind of "demonstration/educational tool" for students and community colleges etc. to show, discuss and learn about some basics of health reforms and politics. The only "risk" I see is that the result is better informed, critical citizens. Regards, Gerd

Re: SimHealth

<Bob_Frankston@frankston.com>

Wed, 23 Feb 1994 00:40 -0400

One general issue of the Sim series is that they portray certain viewpoints of how the world operates and don't pretend to be objective. As noted, there is a danger in using the simulations to understand public policies where just about every parameter is debatable. One benefit is making people appreciate the complexity of interacting systems.

I'm reminded of the Apple ads of a decade ago arguing that pretending to dissect a frog on an Apple][was just as good as cutting open a real frog. It also worth noting that the Psychic Hotlines on the 900 #'s are listed in small type as "for entertainment purposes only". How much of their audience consists of people who are spending \$300/hr just to play a game.

Maxis makes fine software and great games with a number of valid lessons. Too bad schools don't teach much about models vs reality.

Re: Telephone Card Audit Trails (Baube, RISKS-15.57)

"Jonathan I. Kamens" <jik@security.ov.com> Wed, 23 Feb 1994 09:34:56 -0500

What happens when the police arrest a suspect in some crime, find a prepaid phone card on him, take the phone card to the telephone company, and say, "Tell us what calls were made with this card?"

What happens if the enemies of a prominent businessman engaged in private negotiations hire someone to mug him to get his phone card, take the phone card to the telephone company pretending to be the legitimate owner, and claim that it malfunctioned? Will they be able to look at the screen the operator pulls up with the phone numbers called on it? What happens if they don't bother to go to the telephone company directly, and instead just break into the telephone company's computers and read the number off of the stolen card themselves?

This doesn't sound like an "anonymous" system at all.

An alternative system that would do a much better job of protecting users' privacy would be to allow users to type a special code on the pay phone if their card malfunctions while placing a call. That code would cause *that call only* to be recorded in the telephone company's computers. No explicit action by the user means no records in the computer.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@security.ov.com

Re: E-Mail Courtesy (RISKS-15.57)

Jim Haynes <haynes@cats.ucsc.edu> Wed, 23 Feb 1994 09:21:55 -0800

The flip side of this issue (inappropriate questions posted to news or list

server when the questioner should have used the library first) is that it's ego-gratifying to answer questions. So for every simple question there are likely to be dozens of answers, some sent to the asker in private e-mail but many posted back to the list or newsgroup. There is, however a socially redeeming aspect of all this. When dozens of answers are posted many of them will be slightly or completely wrong. One learns, over a period of time, just how unreliable information obtained on the net can be, and whose answers tend to be the most reliable.

Re: E-Mail Courtesy

<Bob_Frankston@frankston.com> Wed, 23 Feb 1994 00:41 -0400

I'd pose the complaint differently. The argument that one should trek miles to the public library to look at the berries on wood pulp before querying the electronic medium is misdirected. There is a valid complaint that reasonable discussions should be stratified according to some measure of common interest or expertise. This is going to be an increasingly serious issue as the network grows, especially in the absence of control mechanisms such as financial incentives and/or an established etiquette.

Asking questions online is more a symptom of the lack of effective information retrieval technology in this medium (net surfing is not the final answer) and is more a teething problem. Yes, deciding not to don ones winter gear and head out into the blizzard is laziness. But it is precisely this laziness that will force the issues and encourage people to make this new medium work. If it breaks, fix it. You can ask people to hold back until the problem is solved but don't blame them for the problem.

I do get a cultural jolt when I use an online catalog only to find I've actually got to find the pbook.

★ Re: Electronic Food Stamps (Kabay, RISKS-15.54)

Colby Kraybill <opus@herschel.unm.edu> Wed, 23 Feb 94 11:12:58 MST

The same program has been floating about New Mexico over a year now. It works very well, I should know, I use it. It is very convenient. My card has a little 'Money card' symbol on the back, name of the service is called Electronic Benefits Transfer or EBT. Some of the propaganda on the card and it's protective sheath:

Warning: It's a crime to illegally use, transfer, acquire, alter or possess food stamps or authorized cards. Persons convicted may be FINED AND/OR IMPRISONED. PENALTIES ARE SEVERE.

(on the card)

This card remains the property of the State of New Mexico Human

Services Department and is subject to the terms and conditions under which it is issued. If found etc.. etc..

In any case, I think that the security of the card is much better than carrying around paper food stamps which someone without the knowledge of your PIN could use.

Colby Kraybill - University of New Mexico - I.F.A.-H.E.P opus@unm.edu

★ Re: International Internet Association (RISKS-15.49)

<jeffporten@aol.com>
Tue, 22 Feb 94 13:53:51 EST

Concerning the Washington Post article about the International Internet Association that was mentioned in <u>RISKS-15.49</u>:

The tone of the original article in the Post and the RISKS followup were along the lines of "Gee, isn't it a shame that this legitimate organization has had its reputation impugned by someone who was took quick on the trigger in his e-mail." There's another side to this story that I'd like to share.

I'm a member of an informal network of organizations in the DC area that work with student and youth activists. We meet for dinner once a month, and a running joke for the last few meetings has been the IIA. Several of us have gotten faxes from the IIA, which promised free Internet access and a forthcoming larger packet of information that never materialized.

Contact was frequent enough to keep us joking and wonder who these people were, but the whole thing had a very fly-by-night feel to it. First off, an organization called the International Internet Association appears out of nowhere... one would have thought that an organization like that would have made itself known *on* the Internet in order to build its reputation. Second, the letterhead consisted of clip art of a world map with IIA typed over it --materials that could have been thrown together in about 15 seconds with no monetary investment, especially since everything we saw arrived by fax.

All of this was merely quaint, until they asked us for a credit-card number for a *free* account. As soon as I saw that, I told the rest of the group to stay as far away from these people as possible; the whole thing just screamed "scam", and I am still not convinced otherwise.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 59

Saturday 26 February 1994

Contents

Microsoft Dinged for \$120 Million

Leaving intelligence to the experts: lie detectors, Clipper

John M. Sullivan Janitor interrupts UPS

Lisa Balbes

Portuguese drug ring ensnared by pager technology

Fernando Pereira

Snag hits Reserve Bank of India's clearing operations

S. Ramani

"Wire Pirates" - article in March 1994 Scientific American

Martin Minow

Van Eck Radiation Helps Catch Spies

Winn Schwartau

Re: Software testing at Sizewell

Dave Parnas

Re: SimHealth

Bill Stewart

Re: The ultimate couch potato

Bear Giles

FLASH: FBI's Draft Digital Telephony Bill: EFF Summary and Analysis

Daniel J. Weitzner

Info on RISKS (comp.risks)

Microsoft Dinged for \$120 Million

"Peter G. Neumann" < neumann@csl.sri.com> Sat, 26 Feb 94 15:18:08 PST

A federal jury in Los Angeles found that Microsoft's MS-DOS 6.0 software infringed upon a Stac Electronics patent for data compression, and awarded Stac \$120M in damages. [San Francisco Chronicle, Business Digest, 24 Feb 19941

Leaving intelligence to the experts: lie detectors and clipper

John M. Sullivan <sullivan@msri.org> Sat, 26 Feb 94 13:10:39 PST

I read this story in Robert Park's "What's New" from opa@aps.org, and am forwarding it because, though it came up in conjunction with the CIA spy, it seems relevant to the discussions of Clipper here.

- -> Recall the 1986 case of Larry Chin, a career CIA analyst and spy
- -> for China; he also fooled the polygraph. In 1983 I was waiting to
- -> testify before the House Security Subcommittee. OTA Director John
- -> Gibbons was summarizing a study of the scientific validity of the
- -> polygraph for the subcommittee. Loosely paraphrased, Gibbons was
- -> explaining that these things couldn't distinguish between a lie
- -> and the sex act. Seated next to me was General Richard Stillwell
- -> (ret.) of the CIA. He had no idea who I was, but he could contain
- -> himself no longer; leaning toward me, Stillwell muttered, "I wish
- -> these damn scientists would leave intelligence to the experts."

Janitor interrupts UPS

Lisa Balbes <balbes@osiris.rti.org>
Thu, 24 Feb 94 14:02:16 -0500

SERVICE INTERRUPTION

Cleanliness is not always the best policy.

There was a short interruption to some ACS services on Thursday, February 24, 1994. The gopher server, postbox, and HomeNet services were offline for about 1 hour at the beginning of the day.

A member of the custodial staff plugged his vacuum cleaner into a power strip attached to our uninterrupted power supply (UPS). Poooooof. Down went several computers and part of the network. Just when you think that you have solved the problem of power outages with a brand new UPS

ACS is working with the custodial services to remedy the problem and prevent future such occurrences.

Lisa Balbes, Osiris Consultants Scientific Software/Technical Writing 2229B Hedgerow Rd, Columbus, OH 43220 balbes@osiris.rti.org 614-442-9850

Portuguese drug ring ensnared by pager technology

Fernando Pereira <pereira@research.att.com> Fri, 25 Feb 1994 23:57:26 -0500

This is 2nd hand from soc.culture.portuguese. Portuguese police found out that

a drug traffic ring used pagers to receive orders from clients, and also to receive announcements of new bulk deliveries (This is a more recent practice in Portugal than in the US, given the relatively recent arrival of pageers there and the less serious drug problem). They arrested one of the drug sellers, took his pager, and started recording the arriving messages. Soon they figured out the code used by the ring, and they caught them all.

Two lessons:

- 1. Physical access to a node is the best way to break into a network.
- 2. Old-fashioned police work can take advantage of the vulnerabilities in criminal activities created by the use of new technology. Even if all the links in that network had been securely encrypted, the method followed by the portuguese police would still work. Food for thought in relation to the current Clipper debate.

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave, PO Box 636 Murray Hill, NJ 07974-0636 pereira@research.att.com

✓ Snag hits Reserve Bank of India's clearing operations

"S. Ramani" <ramani@saathi.ncst.ernet.in> Sat, 26 Feb 1994 23:50:05 +0530

By Business Times Staff, Bombay, 25 Feb 1994

Clearing of cheques at the Reserve Bank of India's national clearing cell (NCC) at Nariman Point came to a half on Wednesday night as a result of a "major fault" in the IBM mainframe computer handling the clearance of magnetic ink character recognition (MICR) cheques. The fault has crippled the reader-sorter machine.

As a result of the breakdown, clearing and settlement of about 10 lakh (i. e. one million) cheques valued at Rs. 1,000 crores (i. e. Rs 10 thousand million, roughly equal to US\$ 300 million) have been held up over the last two days. The disruption has sent corporate houses and the salaried class into a panic as salary payments were due this week.

Sources in the RBI said the fault was yet to be located at the time of going to press today. Personnel from the RBI's Calcutta and Madras Offices and experts from Computer Maintenance Corporation, the maintenance agent of IBM, have been summoned.

The breakdown, according to the sources, was unprecedented in recent times and "the experts are grappling" with the snag since yesterday.

The NCC handles about six lakh cheques each day amounting to a total value of Rs. 1,000 crores. Clearance of high-value cheques (over Rs. 1 lakh) and inter-bank instruments, however, is being carried out unhampered. The worst hit were the public account cheques into which category fall salary cheques and other instruments.

The NCC has been inundated with calls from commercial banks which wanted to find out when normalcy will be restored. As it happens, the snag that stopped the clearing of cheques came at the end of the month and many salaried employees have been left with no choice but to get their cheques discounted.

The back-up programmes which the NCC had were of no avail and the experts had to be summoned. The RBI put up a notice at its Amar Building office and at the NCC yesterday about the snag and said: "Due to a problem with the computer system with the national clearing cell, processing of MICR presentations of yesterday evening (February 23) could not be completed. Member banks are advised that settlement of this clearing will not be accounted for today (February 24). A further communication will follow."

Branches of commercial banks have been advised by their respective zonal offices that "outward MICR clearing could not be presented" yesterday and have been instructed not to release the credits of clearing presented on February 23 and thereafter until further notice.

"The system will have to be rectified, its programme loaded, tested to see whether it can function to its usual capacity and then only the backlog can be cleared," the sources said. The would mean a delay of at least two more days, they added. Loading its programme, incidentally, takes a substantially long period.

"We have made some progress since yesterday and hope to locate the problem by tonight. We expect the machine to start only by tomorrow evening," the sources added.

The mainframe could not load the programme properly on Wednesday night and all efforts by the NCC staff came to naught. Personnel from RBI offices and the CMC had to be flown in yesterday. The RBI is also in touch with IBM personnel who designed the system.

The RBI said in a statement the "computer system developed certain hardware and consequential software problems" on Wednesday. "The problems are being attended to on an emergency basis and the normal cheque clearing and settlement work is expected to resume shortly," the statement said.

High-value cheques and inter-bank payments account for a very large proportion of the clearing settlement in terms of value, the RBI said.

S. Ramani, National Centre for Software Technology, Gulmohar Cross Road No 9, Juhu, Bombay 400 049, India Ph: +91 (22) 620 0590 or 620 1606)

"Wire Pirates" - article in March 1994 Scientific American

Martin Minow <minow@apple.com> Thu, 24 Feb 94 11:09:59 -0800

There is a long article on the "inhabitants of Cyberspace" who "may be

villians, victims, or bystanders" in the March issue of Scientific American, written by Paul Wallich. While the content is probably well-known to Risks readers, the article gives a very good overview of the issues, and people involved.

There are also photos of "Phiber Optik," Dorothy Denning, Donn Parker, and the illustrious editor of this esteemed journal.

Of interest to historians might be the bibliography, listing information available only by FTP or e-mail as if this is the everyday way of locating information in a library.

Martin Minow minow@apple.com

Van Eck Radiation Helps Catch Spies

"Winn Schwartau" <p00506@psilink.com> Thu, 24 Feb 94 14:13:19 -0500

Van Eck in Action

Over the last several years, I have discussed in great detail how the electromagnetic emissions from personal computers (and electronic gear in general) can be remotely detected without a hard connection and the information on the computers reconstructed. Electromagnetic eavesdropping is about insidious as you can get: the victim doesn't and can't know that anyone is 'listening' to his computer. To the eavesdropper, this provides an ideal means of surveillance: he can place his eavesdropping equipment a fair distance away to avoid detection and get a clear representation of what is being processed on the computer in question. (Please see previous issues of Security Insider Report for complete technical descriptions of the techniques.)

The problem, though, is that too many so called security experts, (some prominent ones who really should know better) pooh-pooh the whole concept, maintaining they've never seen it work. Well, I'm sorry that none of them came to my demonstrations over the years, but Van Eck radiation IS real and does work. In fact, the recent headline grabbing spy case illuminates the point.

Exploitation of Van Eck radiation appears to be responsible, at least in part, for the arrest of senior CIA intelligence officer Aldrich Hazen Ames on charges of being a Soviet/Russian mole. According to the Affidavit in support of Arrest Warrant, the FBI used "electronic surveillance of Ames' personal computer and software within his residence," in their search for evidence against him. On October 9, 1993, the FBI "placed an electronic monitor in his (Ames') computer," suggesting that a Van Eck receiver and transmitter was used to gather information on a real-time basis. Obviously, then, this is an ideal tool for criminal investigation - one that apparently works quite well. (From the Affidavit and from David Johnston, "Tailed Cars and Tapped Telephones: How US Drew Net on Spy Suspects," New York Times, February 24, 1994.)

>From what we can gather at this point, the FBI black-bagged Ames' house and installed a number of surveillance devices. We have a high confidence factor that one of them was a small Van Eck detector which captured either CRT signals or keyboard strokes or both. The device would work like this:

A small receiver operating in the 22MHz range (pixel frequency) would detect the video signals minus the horizontal and vertical sync signals. Since the device would be inside the computer itself, the signal strength would be more than adequate to provide a quality source. The little device would then retransmit the collected data in real-time to a remote surveillance vehicle or site where the video/keyboard data was stored on a video or digital storage medium.

At a forensic laboratory, technicians would recreate the original screens and data that Mr. Ames entered into his computer. The technicians would add a vertical sync signal of about 59.94 Hz, and a horizontal sync signal of about 27KHz. This would stabilize the roll of the picture. In addition, the captured data would be subject to "cleansing" - meaning that the spurious noise in the signal would be stripped using Fast Fourier Transform techniques in either hardware or software. It is likely, though, that the FBI's device contained within it an FFT chip designed by the NSA a couple of years ago to make the laboratory process even easier.

I spoke to the FBI and US Attorney's Office about the technology used for this, and none of them would confirm or deny the technology used "on an active case."

Of course it is possible that the FBI did not place a monitoring device within the computer itself, but merely focused an external antenna at Mr. Ames' residence to "listen" to his computer from afar, but this presents additional complexities for law enforcement.

- 1. The farther from the source the detection equipment sits means that the detected information is "noisier" and requires additional forensic analysis to derive usable information.
- 2. Depending upon the electromagnetic sewage content of the immediate area around Mr. Ames' neighborhood, the FBI surveillance team would be limited as to what distances this technique would still be viable. Distance squared attenuation holds true.
- 3. The closer the surveillance team sits to the target, the more likely it is that their activities will be discovered.

In either case, the technology is real and was apparently used in this investigation. But now, a few questions arise.

- 1. Does a court surveillance order include the right to remotely eavesdrop upon the unintentional emanations from a suspect's electronic equipment? Did the warrants specify this technique or were they shrouded under a more general surveillance authorization? Interesting question for the defense.
 - 2. Is the information garnered in this manner admissible in court? I

have read papers that claim defending against this method is illegal in the United States, but I have been unable to substantiate that supposition.

3. If this case goes to court, it would seem that the investigators would have to admit HOW they intercepted signals, and a smart lawyer (contradictory allegory :-) would attempt to pry out the relevant details. This is important because the techniques are generally classified within the intelligence community even though they are well understood and explained in open source materials. How will the veil of national security be dropped here?

To the best of my knowledge, this is the first time that the Government had admitted the use of Van Eck (Tempest Busting etc.) in public. If anyone knows of any others, I would love to know about it.

★ Re: Software testing at Sizewell (RISKS-15.58)

"Peter G. Neumann" < neumann@csl.sri.com> Thu, 24 Feb 94 8:54:34 PST

[Dave Parnas asked me to post the following message from him. It is HIS, not MINE. PGN]

The article in [Nuclear Engineering International, 12/93, p.10, reported by Bob Dolan contained the following assertion, "no other reactor protection system in the world, past or present, has received more attention than the PPS".

Having read the report that was leaked to the BBC and later circulated by other organizations, I see no evidence to support that statement. For example, there have no reports of the software having been subject to a formal (mathematically based) inspection procedure such as the one used for the Nuclear Station at Darlington Ontario.

The leaked report also showed that the authorities were quite prepared to accept a safety-critical software product that had FAILED the majority of its tests on the basis of vague and unsubstantiated claims that the failures were caused by the test harness not the program itself. The report did not indicate that there were any plans to rectify the problems in the test harness and carry out the test properly. There was no indication of how the test cases were selected and whether they were statistically meaningful. I know that in other nuclear plant situations, far more care was taken in the design of testing procedures.

The Sizewellreport was kept secret and I have heard of no plans to have British software experts who are not part of the nuclear industry take part in the evaluation procedure. My experience suggests that, for whatever reasons, "inside experts" tend to be less rigorous and demanding than "outsiders". Organisations tend to pick the experts whom they expect to say what they want to be told. They aren't always right in their predictions, but I have never seen an industry knowingly engage a "loose cannon".

In the Darlington case, reports were not kept secret, and the inspection

process involved many outside consultants.

Sizewell seems to me to provide ample evidence that outside scrutiny, openness, and an active press are essential when there are potential conflicts between short-term financial exigency and safety. Nobody who read that report could have much faith in the authorities who were prepared to accept such test results.

Prof. David Lorge Parnas, Communications Research Laboratory
Department of Electrical and Computer Engineering, McMaster University,
Hamilton, Ontario Canada L8S 4K1

Re: SimHealth

<wcs@anchor.ho.att.com>
Wed, 23 Feb 94 20:16:35 EST

With simulations, good modelling of the real situation and initial conditions is important. With simulation-based propaganda, however, it's also useful to know the biases of the game-writer and the desired conclusion you're supposed to come to :-)

At the Knoxville World's Fair in ?1983, the Tennessee Valley Authority had a simulation game that put you in charge of their power system, letting you pull levers to choose how much power to get from what source, in order to keep enough power for the demand at the best price. The conclusion you were supposed to get was (surprise, surprise), "Use all the hydro power you can, then all the nukes you can, then coal&oil". As a resident of an area whose government gave electrical supply monopoly to the folks who own Three Mile Island and a few other old nuclear plants, I thought they should at *least* have the nuke plants go off-line every once in a while, spending money real fast when they're down:-)

SimCity had a fairly strong bias toward City Planners telling people what to do and making decisions for them instead of letting them do what they want. Is SimHealth similarly biased toward single-decider systems?

Bill Stewart

★ Re: The ultimate couch potato (Balden, RISKS-15.57)

Bear Giles <bear@cs.colorado.edu> 23 Feb 1994 23:27:03 GMT

>... In his view, this would lead to birth of the ultimate couch potato.

The solution is quite obvious, and even environmentally friendly!

Take your standard electronic stationary bike (which uses an electrical generator to produce the current required to run the display) and replace the current display panel with an LCD display and waterproof keyboard.

For even better performance, use logic devices that operate faster if more power is available, so someone really cranking on the pedals will get their job to compile faster than someone who's coasting... and hence get the fat bonus check!

(The home version would determine the recharge period of your weapons (in games) by the amount of power supplied by the user.)

Not only does this ensure that computer users will be among the fittest people on the planet (doing aerobic exercise for 8 hours a day), it would eliminate the need to use fossil fuels to power computer systems, monitors, etc.

Of course, it would require waterproof printouts. But on the other hand, this ensures that long meetings of the programming staff would be a thing of the past....

Bear Giles bear@cs.colorado.edu/fsl.noaa.gov

FLASH: FBI's Draft Digital Telephony Bill: EFF Summary and Analysis

Daniel J. Weitzner <djw@eff.org> Wed, 23 Feb 1994 23:33:00 -0600

Electronic Frontier Foundation Statement on FBI Draft Digital Telephony Bill

EFF has received a draft of the FBI's new, proposed "Digital Telephony" bill. After initial analysis, we strongly condemn bill, which would require all common carriers to construct their networks to deliver to law enforcement agencies, in real time, both the contents of all communications on their networks and the "signalling" or transactional information.

In short, the bill lays the groundwork for turning the National Information Infrastructure into a nation-wide surveillance system, to be used by law enforcement with few technical or legal safeguards. This image is not hyperbole, but a real assessment of the power of the technology and inadequacy of current legal and technical privacy protections for users of communications networks.

Although the FBI suggests that the bill is primarily designed to maintain status quo wiretap capability in the face of technological changes, in fact, it seeks vast new surveillance and monitoring tools. Among the new powers given to law enforcement are:

1. Real-time access to transactional information creates the ability to monitor individuals in real time.

The bill would require common carrier network (telephone companies and anyone who plans to get into the telephone business, such as cable TV companies) to deliver, in real time, so called "call setup information." In the simplest case, call setup information is a list of phone numbers

dialed by a given telephone currently under surveillance. As we all come to use electronic communications for more and more purposes, however, this simple call setup information could also reveal what movies we've order, which online information services we've connected to, which political bulletin boards we've dialed, etc. With increasing use of telecommunications, this simple transactional information reveals almost as much about our private lives as would be learned if someone literally followed us around on the street, watching our every move.

We are all especially vulnerable to this kind of surveillance, because, unlike wiretapping the *content* of our communications, it is quite easy for law enforcement to get permission to obtain this transactional information. Whereas courts scrutinize wiretap requests very carefully, authorizations for access to call setup information are routinely granted with no substantive review. Some federal agencies, such as the IRS, even have the power to issue administrative subpoenas on their own, without appearing before a court.

The real impact of the FBI proposal turns, in part, on the fact that it is easy to obtain court approval for seizing transactional data.

The change from existing law contained in the FBI proposal is that carriers would have to deliver this call setup information *in real time*, directly to a remote listening post designated by law enforcement. Today, the government can obtain this information, but generally has to install a device (called a 'pen register') which is monitored manually at the telephone company switching office.

Access to communication and signalling information for any mobile communication, regardless of location allows tracking of an individual's movements.

The bill requires that carriers be able to deliver either the contents or transactional information associated with any subscriber, even if that person is moving around from place to place with a cellular or PCS phone. It is conceivable that law enforcement could use the signalling information to identify that location of a target, whether that person is the subject of a wiretap order, or merely a subpoena for call setup information.

This provision takes a major step beyond current law in that it allows for a tap and/or trace on a *person*, as opposed to mere surveillance of a telephone line.

3. Expanded access to electronic communications services, such as the Internet, online information services, and BBSs.

The privacy of electronic communications services such as electronic mail is also put at grave risk. Today, a court order is required under the Electronic Communications Privacy Act to obtain the contents of electronic mail, for example. Those ECPA provisions would still apply for the contents of such messages, but the FBI bill suggests that common carriers might be responsible for delivering the addressing information associated with electronic mail and other electronic

communications. For example, if a user connects to the Internet over local telephone lines, law enforcement might be able to demand from the telephone company information about where the user sent messages, and into which remote systems that user connects. All of this information could be obtained by law enforcement without every receiving a wiretap order.

4. The power to shut down non-compliant networks

Finally, the bill proposes that the Attorney General have the power to shut down any common carrier service that fails to comply with all of these requirements. Some have already called this the "war powers" provision. Granting the Department of Justice such control over our nation's communications infrastructure is a serious threat to our First Amendment right to send and receive information, free from undue government intrusion.

The posting represents EFF's initial response to the new FBI proposal. Several documents, including the full text of the proposed bill and a more detailed section-by-section analysis are available by anonymous ftp on EFF's ftp site.

This document is digtel94.announce.

The documents can be located via ftp, gopher, or www, as follows:

ftp://ftp.eff.org/pub/EFF/Policy/Digital_Telephony/digtel94_bill.draft ftp://ftp.eff.org/pub/EFF/Policy/Digital_Telephony/digtel94_analysis.eff ftp://ftp.eff.org/pub/EFF/Policy/Digital_Telephony/digtel94.announce

for gopher, same but replace first part with:

gopher://gopher.eff.org/00/EFF/...

for WWW, same but replace first part with:

http:/www.eff.org/ftp/EFF/...

"I believe in markets doing what they do well, which is to develop technology, and letting citizens do what they ideally do well, which is to set policy."

-Esther Dyson, President, EDventure Holdings, Inc.

The Electronic Frontier Foundation is working to protect your privacy. To help stop Clipper and eliminate export controls on cryptography, support a bill introduced in the House of Representatives, HR 3627. To support the bill, send email to <cantwell@eff.org>.

Daniel J. Weitzner, Senior Staff Counsel, Electronic Frontier Foundation 1001 G St, NW Suite 950 East, Washington, DC 20001 <djw@eff.org>

202-347-5400 (v) 202-393-5509 (f)

*** Send mail to membership@eff.org for information on EFF. ***



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 60

Monday 28 February 1994

Contents

\$1M deposited in bank error

PGN

Another Olympic E-mail Penetration

PGN

The dangers of electronic mail

Rob Hasker

Ex-employee arrested in computer-file theft

Lance Gatrell

How about bounties for inspecting safety-critical software?

Michael Chastain

Reloadable and Smart Cards en route to worldwide acceptance

Gordon Webster and Sree Kumar

FBI Digital Telephony Proposal and PCS mobile phone networks

M. Hedlund

Re: Van Eck Radiation ...

James H. Haynes

Fredrick B. Cohen

Vadim Antonov

Bob Brown

John R Levine

Bill Bolosky

Info on RISKS (comp.risks)

\$1M deposited in bank error

"Peter G. Neumann" <neumann@csl.sri.com> Mon, 28 Feb 94 18:08:00 PST

The Bank of Stockton (California) accidentally turned Mohammed Idrees Kussair's deposit of \$100,000 into \$1M. He assumed that a relative in Pakistan must have wired the money to him, and spent it to pay off rental properties and to take a trip to Pakistan. A San Joaquin County Superior judge ruled that he had not broken any laws, and cleared him of criminal charges. A spokesman for the bank said that the bank intends to sue him. [Source: An AP item in the San

Francisco Chronicle, 11 Feb 1994]

Another Olympic E-mail Penetration

"Peter G. Neumann" < neumann@csl.sri.com> Mon, 28 Feb 94 10:02:04 PST

Misuse of the Olympic E-mail system continued, subsequent to the earlier case reported in <u>RISKS-15.59</u>.

Someone masqueraded as Wayne Abbott, a Canadian TV employee, and sent a nasty E-mail message to Cathy Turner relating to her skating style. [Cathy was disqualified for contact with another skater, after apparently winning the gold in the 1,000-meter speedskate.] [San Francisco Chronicle, 27 Feb 1994, p. C-5]

The dangers of electronic mail

Rob Hasker <hasker@sal.cs.uiuc.edu> Fri, 25 Feb 1994 12:57:45 -0600

Quoting from the Feb. 24 News-Gazette of Champaign-Urbana, Illinois:

"UI student arrested for e-mail threat to Clinton"

URBANA -- A University of Illinois student has been arrested for threatening the life of President Clinton, U.S. Attorney Frances Hulin announced today.

Christopher James Reincke, 18, of Townsend Hall, Urbana, allegedly sent an electronic mail message to the White House on Dec. 4 threatening Clinton, Hulin stated in a press release.

The message read: "I am curious, Bill, how would you feel about being the first president to be killed on the same day as his wife ... It would be best, I think, to not continue with your immediate plans. Perhaps a vacation. You will die soon. You can run, but you cannot hide."

The message was signed "Overlord" and purported to be from "Allmighty@Never.Gonna.Catch.Me."

Reincke appeared before U.S. District Judge Harold A. Baker in Danville today and was released on his own recognizance.

Hulin said the charge resulted from an investigation by the Secret Service and the UI police.

Investigators determined the message originated at the UI, and a computer trace identified Reincke as the apparent author, Hulin said.

While being questioned by agents, Reincke admitted he had sent the message, according to the press release.

(Local news reports suggest that the student intended this to be a practical joke. As I see it, the risk is in assuming that it doesn't really matter what you say by email.)

Rob Hasker hasker@cs.uiuc.edu

Ex-employee arrested in computer-file theft

Lance Gatrell <gatrell@aragtap.den.mmc.com> Mon, 28 Feb 94 09:30:50 MST

Denver Post, p. 1C, Feb. 25, 1994

A former employee of a Boulder [Colorado] computer software company was arrested yesterday for fraudulently transferring 122 computer files worth \$915,000 just before leaving his ex-employer, the FBI said in Denver federal court documents. Liaosheng Wang, also known as Andrew Wang, of Westminster, was arrested by FBI agents for allegedly stealing the computer files, including important "source code files," from Ellery Systems Inc., where he worked as a design engineer from December 1990 until his resignation this month.

In a complaint filed in U.S. District Court in Denver, FBI special agent John Gedney said Wang may have stolen the files after twice being denied promotions at the Boulder company late last month. ... Wang apparently transferred the files from his account at Ellery Systems to Internet, a global computer network, the complaint said. From Internet, Wang was able to communicate from his computer at Ellery Systems with a computer at Unidata Inc., a Denver company. [sic]

The FBI is continuing its investigation to determine if Wang was trying to sabotage his former employer or transferred the information for a fee. "Everything that was transferred was confidential property," said Jeff Jordan, an Ellery vice president. "It was the source code for our product and we intend to get it back." [...]

Geoffrey Shaw, Ellery Systems' chief executive officer, told the FBI that Wang had no authority to transfer the files to Unidata, particularly since they contained a proprietary program that had been copyrighted.

If convicted of wire fraud, Wang could be sentenced to up to five years in prison and fined up to \$250,000.

How about bounties for inspecting safety-critical software?

Michael Edward Chastain <mec@shell.portal.com> Sun, 27 Feb 1994 00:14:22 -0800

After reading a recent RSISKS article about validating the Sizewell B PPS software, I was struck by an idea: how about a bounty for inspecting safety-critical software?

Here's the plan: the government organization which is purchasing the safety-critical software publishes the specification, the entire source code as delivered by private contractors, and technical documentation

on the hardware environment. It then offers a bounty to any party anywhere who demonstrates a logical error in the software. The bounty would be funded by reductions in money paid to the original contractors.

Finding a bug is much harder than demonstrating that one has found a bug. Bounty hunters would have an incentive to deploy whatever technology they found useful in finding errors.

Michael Chastain mec@shell.portal.com

Reloadable and Smart Cards en route to worldwide acceptance

Gordon Webster <pwajam!gordon@uunet.UU.NET> Fri, 25 Feb 94 17:19:31 est

Of late there have been quite a few articles in the RISK forum regarding Smart/Reloadable Cards and issues surrounding their incipient risks. The impression (whether right or wrong) is that most readers (or respondents) are not aware of the level of acceptance that this technology have outside of North America. While the potential risks of the cards are legion, I will not attempt to address them at this point, but merely attempt to touch the tip of iceberg and illustrate the impact having outside of North America.

The kind of chargeable card described in John Gray's item in RISK issue #49 has been available in Japan and some other parts of Asia for at least a year. The cash the card is charged with can be spent at any retail outlet equipped with a simple PoS-type terminal; and the card can be "re-loaded" with cash at ATMs, by a simple transfer from a current or savings account held by the same holder.

Both mag-stripe and embedded-chip versions of the card are in commercial use. The embedded-chip versions are usually multi-function cards (i.e., they can be used for other purposes as well as that of an electronic wallet).

Countries in which reloadable card programs (or pilot programs) exist include: Singapore, Japan, France and South Africa. The cards used are mostly embedded-chip cards, not mag-stripe based. These cash cards are loaded electronically in machines similar to ATMs, by transfer from chequing or savings accounts.

Cards can be used at any retailer with a reading device. The reading device deducts purchase price, issues a receipt, and shows the balance remaining on the card. Some of them (not all) are PIN-activated (RISK readers take note). When the balance on the card is exhausted the card is taken back to the issuing bank or a retail machine for replenishment.

In Japan, the use of the cards apparently has been growing quickly, there is some political pressure to regulate the business, because it is seen as cutting into the Bank of Japan's sole right to issue bank-notes. There is talk of regulations to force issuers to deposit a specified percentage of the money circulating on such cards with the central bank, or to charge a consumption tax on such transactions, the money to go into a central fund which would

reimburse card-holders in case the issuing institution went belly-up.

The Japanese are fairly far along in terms of acceptance of the cards, some of the applications are as follows:

- NTT (the Japanese equivalent of AT&T) is a large proponent of the use of the cards for making pay phone calls. They have found their usage quite profitable as they have found that callers using such cards talk 20-40% longer on the phone, maybe because they don't have to fumble for coins or replacement cards.
- Other Japanese retailers who accept such cards include the railways, buses and taxis, car washes, highway toll booths, fast-food outlets and even video-game arcades.
- One of the last bastions in Japan to hold out against such cards gave in not long ago. You can now use them at Buddhist temples, to make donations. An argument between religious and tax establishments now threatens. Temples have been tax-exempt so far, but the tax authorities do not want to exempt them from the consumption tax on the use of cards.

Another country which has launched a smart card scheme is Guatemala, no less. The scheme in Guatemala is called Credisa, the card is called Elite, and the launching bank is a new retail bank called MultiBanco. The hardware and software are being provided by GemPlus, the same (French) vendor who provided the hardware for the French reloadable card pilot.

In Guatemala, I believe the major incentive for smart cards is the poor telecomms infrastructure, which places limits on on-line authorization capability.

Gordon Webster - Price Waterhouse Assoc. Jamaica - gordon@pwajam.uunet Sree Kumar - Price Waterhouse Assoc. Jamaica - sree@pwajam.uunet

FBI Digital Telephony Proposal and PCS mobile phone networks

"M. Hedlund" <hedlund@netcom.com> Mon, 28 Feb 1994 11:32:59 -0800 (PST)

This article elaborates on part of the EFF statement issued last week concerning the FBI's proposed Digital Telephony wiretap bill. The EFF condemned the bill, which enlarges law enforcement powers of surveillance, granted by wiretap laws, by adding tracking ability. Addressed herein is point two of the EFF statement, concerning the surveillance of mobile communicators, such as cellular phones, Personal Communications Services (PCS) and laptop computers. PCS mobile phones create severe privacy risks for future phone users, especially under the FBI's proposal; and these risks strongly support the EFF's position.

The FBI asserts that their proposal adapts existing wiretap laws to account for emerging communications technologies. Wiretap laws have not adequately covered mobile communications, and the FBI is correct to assume

that some revisions will be necessary to adequately balance law enforcement needs with the privacy rights of mobile phone users. Their proposed revisions, however, do not simply provide for wiretap; instead, the FBI seeks to expand wiretap laws, allowing law enforcement officers to track the signalling information of mobile communications users.

The EFF believes that the FBI proposal would create an enormous hole in the privacy rights of individuals suspected of crimes. Their statement notes:

It is conceivable that law enforcement could use the signalling information to identify the location of a target.....This provision takes a major step beyond current law in that it allows for a tap and/or trace on a *person*, as opposed to mere surveillance of a phone line.

This fear is completely realistic. It is not simply "conceivable" that the FBI's proposal would allow law enforcement to surveil the location of a target -- positioning technology is a planned part of PCS networks, one of the technological advances anticipated by the proposal. Similar positioning technology is planned for cellular phones, as well.

PCS advances cellular phone technology by integrating mobile communications with other phone networks, and by expanding the services and quality mobile phones can offer. Most PCS proposals involve three forms of mobility: terminal mobility, the ability to make and receive calls at any location, and the ability of the phone network to track the location of the mobile phone; personal mobility, the ability of the user to be reachable by a single phone number at all times; and service mobility, the ability of the user to access CLASS(sm)-like features, such as Call Waiting and Caller ID, from any phone they use.

The FBI proposal requires phone companies, when presented with a wiretap order, to transmit the content and the signalling, or "call setup information," from the tapped phone to law enforcement officers. With a wireline phone, such as a residence phone line, call setup information would comprise only the originating and dialled phone numbers, as well as billing information (such as the residence address) for the call. Because of the wireless aspect of PCS, however, call setup information for a PCS phone includes very detailed information on the location and movement of the caller.

PCS mobile phones will connect with the phone network via "microcells," or very small receivers similar to those used for cellular phones. While a cellular network uses cells with up to an 8 to 10 mile radius, PCS networks will use microcells located on every street corner and in every building. The call setup information for a PCS call would include the microcell identifier -- a very specific means of locating the user. An order for a PCS wiretap would allow law enforcement officers to receive a detailed, verifiable, continuous record of the location and movement of a mobile phone user.

These phones are also likely to "feature" automatic registration: whenever the PCS mobile phone is on (in use or able to receive calls), it will automatically register itself with the nearest microcell. Law enforcement

agencies, able to track this registration, would have the equivalent of an automatic, free, instantaneous, and undetectable global positioning locator for anyone suspected of a crime.

PCS tries to improve on cellular phone privacy and security by incorporating cryptographic techniques. Encryption could not only create a secure phone conversation, but could also (coupled with use of a PIN number) insure that only a valid subscriber could make calls on a particular phone, preventing fraudulent calls on stolen phones. An additional phone-to-network authentication could prevent fraudulent calling through a "masquerade" phone designed to simulate a user's registration.

But the FBI proposal would require that such encryption be defeatable in wiretap circumstances. As the proposal stands, this form of weak encryption is distinguishable from the Clipper Chip because the phone companies, not a key escrow arrangement, enable law enforcement access; but it is entirely possible that the Clipper Chip could be used as the encrypting device. In either circumstance, PCS encryption could be compromised by careless or malicious law enforcement officials. Perhaps it is time for Phil Zimmerman and ViaCrypt to begin work on PGPCS -- and let us all hope we are so lucky.

The cellular phone market is tremendous, and analysts believe that the PCS market, incorporating both voice and data communications, will be even larger. Coupled with the FBI's Digital Telephony proposal, PCS raises many privacy and security risks, making the EFF's condemnation of the FBI proposal all the more appropriate.

CLASS is a service mark of Bell Communications Research (Bellcore).

For more information:

- * Bellcore Special Report SR-INS-002301, "Feature Description and Functional Analysis of Personal Communications Services (PCS) Capabilities," Issue 1, April 1992. Order from Bellcore, (800) 521-CORE (2673), \$55.00.
- * GAO report GAO/OSI-94-2, "Communications Privacy: Federal Policy and Actions," November 1993. Anonymous FTP to cu.nih.gov, in the directory "gao-reports".
- * EFF documents, available via anonymous FTP or gopher: ftp://ftp.eff.org/pub/EFF/Policy/Digital_Telephony

[*The New York Times* today has a front-page article by John Markoff, entitled "Price of Technology May Be Privacy". I first saw a version of it in today's *San Francisco Chronicle*, although as seems typical of the Chron they truncated it after 11 of its 34 paragraphs. At least they mentioned Markoff this time, which they frequently do not do! PGN]

Re: Van Eck Radiation and Clipper and Wiretapping

"James H. Haynes" <haynes@cats.ucsc.edu> Mon, 28 Feb 1994 11:15:30 -0800 (PST)

It just struck my irony bone that we have the Feds on the one hand wanting to install leaks in encryption and communication switching; and we have the FCC regulating things like PCs so they don't radiate interfering signals. When will FCC be ordered to "get with the program" and _require_ that PCs and monitors radiate enough so the snoops can do their jobs?

✓ Van Eck Radiation (Schwartau, RISKS-15.59)

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Sat, 26 Feb 94 22:26:48 PST

The contention that this is a Van Eck device is ludicrous! You don't need to use radiated signals if you place a bugging device in the computer. You simply listen to the information and transmit it over a normal radio channel.

> The device would work like this:

This is not how Van Eck's mechanism worked. It exploited the normal radiated signals, not those created by a bugging device.

- > I spoke to the FBI and US Attorney's Office about the technology used for
- > this, and none of them would confirm or deny the technology used "on an
- > active case."

Now that's a journalistic confirmation if I ever heard one!

- > To the best of my knowledge, this is the first time that the Government had
- > admitted the use of Van Eck (Tempest Busting etc.) in public. ...

Since when is a refusal to comment an admission?

If the point of the article is to assert that there are radiated signals from video screens that can be used at a distance to observe the content of the screens, of course there is. If you want confirmation, why not go and buy the 100 dollars of equipment required to do it yourself?

Re: Van Eck monitoring

Vadim Antonov <avg@titan.sprintlink.net> Sat, 26 Feb 1994 19:45:47 -0500

First of all, reception of a signal from computer screen is much easier than it seems due to the fact that images are mostly static; i.e., the same pattern of radiation will be repeated many times allowing for digital accumulation of the signal (it works the same way for astronomers who are able to resolve very dim objects by collecting "random" photons for a long time). Interferometry (i.e., simultaneous reception of the signal from several distant points and

multiplying the received signals delayed to compensate for the propagation delays) can also be a very useful tool to sort out weak signal coming from a single source with known location from random electromagnetic noise.

Also, cleaning up the signal using spectral analysis (FT, etc.) should work great because the spectre of the source signal is discrete (i.e., all frequencies are derived from a single stable oscillator's frequency by dividing it by small integer numbers).

Add directed antennae or (even better) phased antennae arrays and you got the picture...

It's nothing more than methods very well known in optical and radio astronomy so the special services don't have to bother me:-)

--vadim

✓ Van Eck Radiation Helps Catch Spies (?!?)

Bob Brown

Sun, 27 Feb 94 10:41:47 EST

Winn Schwartau [RISKS-15.59] headlined his message "Van Eck in Action" suggesting that the FBI used electromagnetic eavesdropping in developing their case against Aldrich Ames. Later Schwartau quotes the FBI's own affidavit as saying that 'the FBI "placed an electronic monitor in his (Ames's) computer," suggesting that a Van Eck receiver...'

It's time for someone to shout "Occam's Razor!" If the FBI placed anything "in" Ames' computer, it needn't have been anything as complicated as a receiver that sucked keyboard strokes or video pixels out of the electronic chaos that's inside a computer case. A sophomore EE student could design a high-impedance device to pluck video and keyboard signals directly off their respective connectors and relay them onward. Such a gadget would be much simpler, and therefore more reliable than a Van Eck receiver.

On the other hand, the FBI could have simply copied the contents of Ames' hard disk with something like LapLink. They're (understandably) not talking.

★ Re: Van Eck Radiation Helps Catch Spies, maybe not

John R Levine <johnl@iecc.com> Sun, 27 Feb 94 15:40 EST

>On October 9, 1993, the FBI "placed an electronic monitor in his (Ames') >computer," suggesting that a Van Eck receiver and transmitter was used >to gather information on a real-time basis.

I don't know about you, but if I were able to stick a bug inside the computer, I'd attach it directly to the keyboard and video ports. Why fool around trying to reconstruct a signal, when a wire containing the signal itself is

half an inch away?

Do we have here a risk of technophilia? Even if I couldn't get inside the house, it's quite possible that a conventional camera looking through a window could see enough of the the screen and keyboard to gather useful information.

John Levine, johnl@iecc.com, jlevine@delphi.com, 1037498@mcimail.com

Re: Van Eck Radiation Helps Catch Spies

Bill Bolosky <bolosky@microsoft.com> Mon, 28 Feb 94 13:44:28 TZ

A case recently came up in Washington State that is related to the question of the legality of using Van Eck radiation emitted from a residence as a survelience technique.

In the incident in question, a person was suspected of growing marijuana in his home, using grow lights. However, there was insufficient evidence to get probable cause for a search warrant. So, without a warrant, the police stood in the street and used an IR detector on the house. They determined that the house was emitting radiation that was consistent with grow lights, and used this evidence as probable cause to get a search warrant. In the ensuing search, the house was found to contain marijuana and the homeowner was convicted.

He appealed his conviction on the grounds that the use of the IR detector constituted a search of his home, for which a warrant was required; evidence from this illegal search could not be used as probable cause for a warrant. The Washington State Supreme court agreed with the defendant, ruled the search illegal and overturned his conviction. They said that non-visible radiation emanating from a home is not the same as, say, leaving a window open, and that a reasonable expectation of privacy existed for such radiation.

I would imagine that this legal precident would also preclude the use of Van Eck radiation detectors in the state of Washington without a search warrant. Of course, in the Ames case such a warrant almost certainly had already been obtained based on other probable cause, and so this wouldn't be a valid defence for Ames.

Bill Bolosky bolosky@microsoft.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 61

Thursday 3 February 1994

Contents

More on the \$1M deposited in bank error

Raju Varghese

Internet Trojans

Mich Kabay

Biometrics

Paul Robinson

Re: Aldrich Ames and the Clipper Project...

Peter Wayner

Some Thoughts on Clipper, NSA, and one key-escrow alternative

Jim Bidzos

Algorithms have unclear boundaries

Mike Crawford

Response from Cambridgeshire Constabulary

Lawrence Kestenbaum

Re: Threatening E-mail

Peter B Ladkin

Re: Bounties for Safety-Critical Software

Peter B Ladkin

Info on RISKS (comp.risks)

✓ More on the \$1M deposited in bank error (RISKS-15.60)

Raju Varghese <raju@inso.pr.net.ch> Tue, 1 Mar 94 19:22:37 +0100

>The Bank of Stockton (California) accidentally turned Mohammed Idrees >Kussair's deposit of \$100,000 into \$1M. ...

Did the bank say why they converted \$100,000 to \$1,000,000? Could it be due to the following: in India & Pakistan the placement of commas on large numbers is different from the west. The power-of-ten table and their names are shown below:

ten

10

hundred 100 thousand 1000 ten thousand 10,000 one lakh 1,00,000 ten lakhs 10,00,000 one crore 1,00,00,000

Could he have deposited a check which was made out for \$1,00,000 but got `corrected' by the bank because an `obvious' error was made in the number of zeroes.

Just a wild guess... Raju Varghese raju@inso.pr.net.ch

[No lakh of confusion. Mighty lakh arose? A rose is arose is arisen. PGN]

✓ Internet Trojans

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 28 Feb 94 21:35:19 EST

>From the Washington Post newswire, 17 February 1994, via Executive News Service (GO ENS) on CompuServe:

"Break-Ins Prompt A Search for Better Computer Security By John Burgess, Washington Post Staff Writer

Since the dawn of the electronic age, the computer password has been a trusted guardian of secrets large and small. For many people, obtaining their own password became a rite of initiation into computer culture itself. Now, growing numbers of security experts feel that the password in its common form is too old and unsophisticated for the job."

The author continues with the following key points:

- The IAB (Internet Architecture Board) is now arguing for a change to alternative methods of identification and authentication (I&A).
- o Proposals include hand-held one-time password generators and smart cards.
- Concern is growing over the practice of sending cleartext passwords through unencrypted communications channels.
- o Trojan Horse programs can capture unencrypted passwords and store them for misuse by criminal hackers.
- o The most recent attack described in a CERT-CC (Computer Emergency Response Team Coordination Center) Advisory involved a Trojan.
- o There is as yet no evidence of widespread use of the captured passwords.
- o Another approach to I&A is the challenge-response system, in which the computer logging on to another system has to perform calculations

based on data and algorithms stored on the client and the server machines.

- Other methods focus on biometric I&A.
- In general, current use of passwords needs to be improved: users should select passwords with strong random components to prevent dictionary attacks and should guard their passwords closely against inadvertent or deliberate disclosure.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

✗ Biometrics

Paul Robinson <PAUL@TDR.COM> Wed, 2 Mar 1994 22:42:24 -0500 (EST)

'Biometrics' refers to the use of physical charactersistics as identification. Human beings use this in that when we see a friend, we identify them by face, size, hair color, etc. Changes in Biometric data usually return an identification when positive ("Are you losing weight?", "Gee your hair looks teriffic") while negative changes are usually not stated publicly ("I see he's getting married, but his bride-to-be looks somewhat plumper than before; perhaps they _had_ to...").

However, when someone else needs to identify you and doesn't know you, they usually have to rely on authentication. Usual forms of authentication are various forms of paper, photographic/multimedia, and/or magnetic authentication issued by a government or trusted third-party.

With the increased sophistication of duplicating equipment, relyance on documentary authentication is becoming unreliable. Witness the fact that anyone giving out a social security number is presumed to be the holder of that number. When they aren't, the actual holder is usually chagrinned to find out how much expense and damage they have to suffer to rectify the situation.

With this, various organizations are working on means of real-time automatic biometric identification of individuals. The implications of this can be both good and bad. As the actual article is rather complicated, I'll summarize it in a separate article here.

The dangers to people is that if, for example, biometric photographic measurements are used, that real-time tracking of people could be done as the technology gets cheaper. Further, you may never even know that you've been tracked unless and until something happens that it comes to your attention.

Paul Robinson - Paul@TDR.COM

★ Re: Aldrich Ames and the Clipper Project...

Peter Wayner <pcw@access.digex.net> Thu, 3 Mar 1994 12:54:01 -0500

What does the Aldrich Ames Spy Case mean about Clipper? In an earlier posting, I thought it just proved that people could be bought and this meant that the Clipper escrow keys weren't that safe.

Yesterday, I spoke with a Clipper Fan who said that Ames was an isolated case and Ames wouldn't have a need-to-know about Clipper keys. I'm not so sure.

The fact is that someone in Ames's position would be one of the first people who would need access to the Clipper keys. The Department of Justice and other parts of the government have already placed large orders for the Clipper capable phones. The anti-US government spies would be operating in this arena. This is precisely where Ames should have been looking for spies to counter. If everyone at the DOJ and the FBI is going to be using Clipper, then Ames would be one of the first with a need-to-know.

The private sector response is much cooler and local cops will probably go years before needing access to Clipper keys.

Now consider another important fact. The Escrow Key Kops won't have a list matching names with Clipper Chip ID numbers in order to prevent them from abusing their keylist. (Memo to NIST: Don't measure response time to tap requests in Keystones.) They won't be able to tell if a spy in Ames position is asking for the Clipper Key to some long sought after mole or the target dictated by his foreign masters. Such a spy could have complete and total access to any Clipper-protected conversation they wanted.

People designing the Clipper system must not only consider the security of the two Escrow Key Centers, but they must also look at who gets access to the keys. This is going to be the weak link and if Clipper becomes standard there will be plenty of potential weak links around.

✓ SOME THOUGHTS ON CLIPPER, NSA, AND ONE KEY-ESCROW ALTERNATIVE

Jim Bidzos <jim@RSA.COM> Thu, 3 Mar 94 09:43:58 PST

In a recent editorial, Dr. Dorothy Denning of Georgetown University argued in support of the U.S. government's proposed Clipper Chip, a security device that would allow law enforcement to decipher the communications of users of such devices.

Dr. Denning attempts to argue that Clipper is necessary for law enforcement agencies to be able to do their job. I'm not going to argue that one; there are plenty of people who can argue that compromising privacy for all citizens in order to aid law enforcement is a bad idea more effectively than I, particularly in the Clipper case, where the arguments from law enforcement are dubious at best. (The current justification is inadequate; there may be better reasons, from a law enforcement perspective, but we haven't heard them yet.)

Without doubt, law enforcement and intelligence are huge stakeholders in the debate over encryption. But every individual and corporation in the U.S. must be included as well. Are NSA's actions really in the best interests of all the stakeholders? Are there alternatives to the current key escrow program?

If one steps back and looks at what has happened over the last few years, one might well question the approaches, if not the motivation. (I believe it may even be possible to conclude that Clipper is the visible portion of a large-scale covert operation on U.S. soil by the National Security Agency.)

Over a number of years, through their subversion of the Commerce Department (who should be championing the causes of U.S. industry, not the intelligence agencies), NSA has managed to put many U.S. government resources normally beyond their control, both legally and practically, to work on their program of making U.S. and international communications accessible.

The first step was the MOU (Memorandum of Understanding) between NIST NSA. This document appears to contravene the provisions of the Computer Security Act of 1987, the intent of which was to give NIST control over standards-making for the unclassified government and commercial sectors. The MOU essentially gave NSA a veto over any proposals for crypto standards by NIST.

By using the standards making authority of the National Institute of Standards and Technology (NIST), NSA is attempting to force the entire U.S. government to purchase Clipper equipment since only NIST-standard equipment may be purchased by government agencies. This purchasing power can then be used to force U.S. manufacturers to build Clipper products or risk losing government business. (GSA is currently questioning NSA's authority to control government-wide procurement, and should continue to do so.) This of course not only subsidizes Clipper products, but could make Clipper a de facto standard if the costs associated with alternatives are too high. These costs to industry, of ignoring Clipper, come in the form of lost government market share, costly support for multiple versions of incompatible products, and non-exportability of non-Clipper products.

It also appears that NSA is desperately seeking a digital signature standard that would force users to take that signature capability wrapped up with a Clipper chip. If this is the case, as it appears to be, then NSA has is trying to use what is probably the most powerful business tool of the information age as a means to deny us its benefits unless we subsidize and accept Clipper in the process. This would, if true, be an unprecedented abuse of government power to influence U.S. industry and control individual privacy. (Clipper is part of a chip called Capstone, which is where their proposed digital signature standard would be used.)

The overall cost of these policies is unknown. We only know that NSA has spent a considerable amount of money on the program directly. Other costs are not so obvious. They are:

- * A burdened U.S. industry, which will have to build multiple products or more expensive products that support multiple techniques;
- * A low-intensity "trade war" with the rest of the world over

encryption;

- * Lost sales to U.S. companies, since international buyers will surely go to non-U.S. suppliers for non- Clipper encryption, as may buyers in the U.S.;
- * Potential abuses by government and loss of privacy for all citizens.

Does NSA truly believe they can displace other methods with Clipper? With over three million RSA products, the technology they feel threatened by, in use in the U.S. today? Not likely; therefore, they have already decided that these costs are acceptable even if they only delay the inevitable, and that U.S. industry and U.S. taxpayers should bear these costs, whatever they are. This policy was apparently developed by unelected people who operate without oversight or accountability. Does the White House really support this policy? (Does this all sound familiar?)

It has been rumored that NSA will gain support from foreign governments for escrow technology, especially if "local control" is provided. Even if NSA can convince their sister organizations around the world to support key escrow (by offering Clipper technology with a do-your-own-escrow option), will these other governments succeed in selling it to their industry and citizens? Most countries around the world have much stronger privacy laws and a longer history of individual privacy than the U.S.

WHY AGAIN WHEN IT DIDN'T WORK THE FIRST TIME?

Many seem to have forgotten or are not aware that the Clipper program is not new, and it's also not the first time NSA has attempted to force communications security on U.S. industry that it could compromise. In the mid-80's, NSA introduced a program called the Commercial COMSEC Endorsement Program, or CCEP. CCEP was essentially Clipper in a black box, since the technology was not sufficiently advanced to build lower-cost chips. Vendors would join CCEP (with the proper security clearances) and be authorized to incorporate classified algorithms into communications systems. NSA had proposed that they themselves would actually provide the keys to end-users of such systems. The new twist is access by key escrow.

To see how little things have changed, consider this quote: "...RSA Data Security, Inc. asserts that since CCEP-2 is not published and therefore cannot be inspected by third parties, the NSA could put a 'trap door' in the algorithm that would enable the agency to inspect information transmitted by the private sector. When contacted, NSA representative Cynthia Beck said that it was the agency's policy not to comment on such matters." That was in 1987. ("The Federal Snags in Encryption Technology," Computer and Communications Decisions, July 1987, pp. 58-60.)

To understand NSA's thinking, and the danger of their policies, consider the reply of a senior NSA official when he was asked by a reporter for the Wall Street Journal if NSA, through the CCEP program, could read anyone's communications: "Technically, if someone bought our device and we made the keys and made a copy, sure we could listen in. But we have better things to do with our time." (The Wall Street Journal, March 28, 1988, page 1, column 1, "A Supersecret Agency Finds Selling Secrecy to Others Isn't Easy," by Bob Davis.)

Another NSA official, in the same Journal story, said "The American Public has no problem with relying on us to provide the technology that prevents the unauthorized launch of nuclear weapons. If you trust us to protect against that, you can trust us to protect private records." Remember that the Cold War was still on at that time. Maybe they're not so busy today.

Law enforcement and intelligence gathering are certainly impeded by the use of cryptography. There are certainly legitimate concerns that these interests have. But is the current approach really the way to gain support? People with a strong military and intelligence bias are making all the decisions. There seem to be better ways to strike a balance.

AN ALTERNATIVE PROPOSAL

One approach would be to have NIST develop a standard with three levels. The first level could specify the use of public-key for key management and signatures without any key escrow. There could be a "Level II" compliance that adds government key escrow to message preparation. "Level III" could be key escrow controlled by the user, typically a corporation. Would this work? The first level, meeting the standard by itself, would back up the government's claim that key escrow is voluntary; if I want privacy and authentication without key escrow, then I can have it, as the government has claimed I can. Actions speak louder than words.

Why would any vendors support Level II? They would find a market in the government. (I would certainly like our public servants to use key escrow, just as I want work product paid for by my corporation to be accessible.) So the government can still influence the private sector by buying only products that include Level II compliance. Also, Level II products would be decontrolled for export. The market can decide; vendors will do what their customers tell them to. This satisfies the obvious desire on the part of the government to influence what happens, as a consumer.

Level III would allow any user to insert escrow keys they control into the process. (Level II would not be a prerequisite to Level III.) My company may want key escrow; I, as an individual, may want to escrow my keys with my attorney or family members; a standard supporting these functions would be useful. I don't necessarily want or need the government involved.

NIST already knows how to write a FIPS that describes software and hardware implementations, and to certify that implementations are correct.

This approach certainly isn't perfect, but if the administration really believes what it says and means it, then I submit that this is an improvement over a single key escrow FIPS foisted on everyone by NSA, and would stand a much better chance of striking a workable balance between the needs of the government and the right of individuals to privacy. Therefore, it RISKS much less than the current plan.

The real problem with the way NSA works is that we don't find out what they're really doing and planning for decades, even when they're wrong. What if they are?

In the 60's and 70's, the CIA was out of control, and the Congress, after

extensive hearings that detailed some of the abuses of power by the CIA, finally moved to force more accountability and oversight. In the 80's and 90's, NSA's activities should be equally scrutinized by a concerned Congress.

Algorithms have unclear boundaries

Mike Crawford <crawford@scipp.ucsc.edu> Tue, 1 Mar 1994 12:44:05 -0800

This is a letter I just sent to the Patent and Trademark office in which I discourage software patents because the boundaries between components of software machines are not well defined.

Mail your software patent comments to comments-software@uspto.gov.

Mike Crawford | Author of the Word Services Apple Event Suite.

crawford@scipp.ucsc.edu | Free Mac Source Code: ftp sumex-aim.stanford.edu

| get /info-mac/dev/src/writeswell-jr-102-c.hqx

Dear Patent Commissioner,

I object to the existence of software patents. I object for many reasons, but an argument you may not have heard before is that computer algorithms do not have clear boundaries. Thus it is not possible, or not feasible, to prove that a particular software product has not used some algorithm which has been patented. This problem is due to the very nature of software, so I feel that patents should not apply to software.

It is somewhat difficult to express this concept clearly, but consider this:

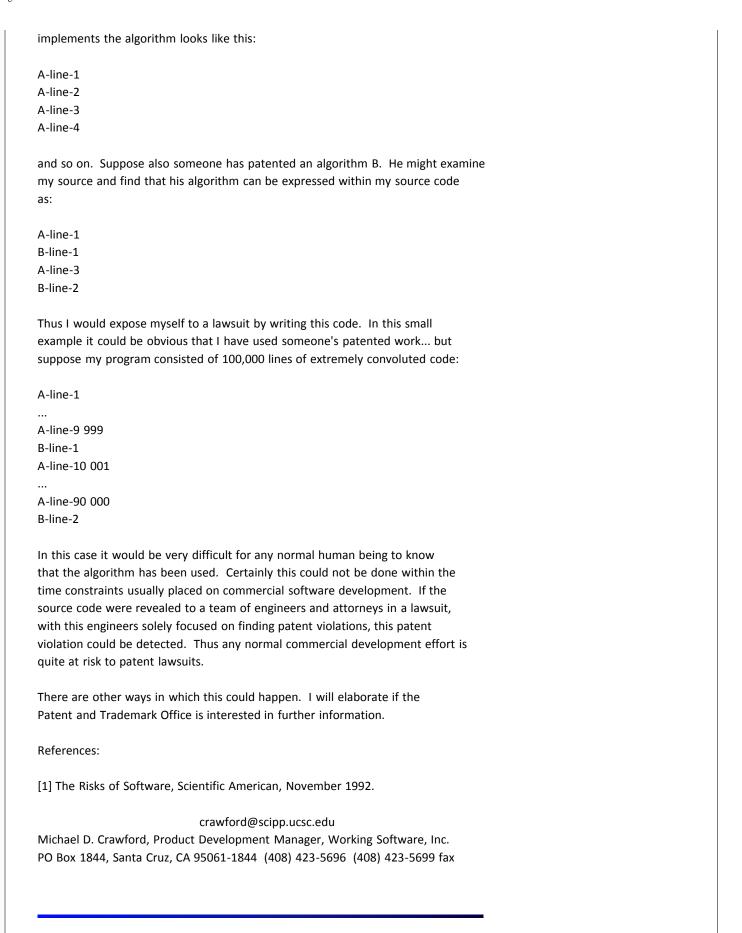
A mechanical device, made of metal, has hard surfaces. There are clearly defined boundaries between metal parts. It is clear where one device stops and another starts in physical space - or at least one can take a machine apart to determine this.

Thus one can examine a machine for patent violation by taking it apart and looking at the pieces.

This is not always the case with software. Computer programs are usually implemented as some sort of "virtual machine", in which mechanistic concepts are used to guide the construction of the software, but computer programs have the peculiar property of having no boundaries. (Or, if you prefer, soft and penetrable boundaries.)

This is a problem for software reliability, for example: any line in a computer program has the capacity to reach out and destroy any other line. Thus software programs are inherently unreliable. [1] If this could happen in a mechanical system, a poorly molded windshield wiper might reach into the engine and throw a piston rod. This does not happen to mechanical systems, but it is a daily problem in my work as a programmer.

Now, suppose I devise an algorithm, let us call it A. The source code that



Response from Cambridgeshire Constabulary

Lawrence Kestenbaum <22914LCK@msu.edu>

Tue, 01 Mar 94 17:03:56 EST

From: Lawrence Kestenbaum School of Criminal Justice Michigan State University 22914LCK@msu.edu

This is in relation to the recent article in RISKS by Ross Anderson. He described the case of John Munden, an English police constable who complained of unauthorized transactions appearing on his bank statement and (without any other real evidence) was tried and convicted of ATM fraud.

I was sufficiently outraged to (as Ross suggested) send a letter to the Chief Constable of the Cambridgeshire Constabulary, expressing my deep concern.

I enclosed a copy of the RISKS report and stated that my opinion was based on this information.

Here is the reply I received today, dated 18 February 1994:

Dear Sir,

I acknowledge receipt of your letter concerning the case of Police Constable John Munden who was recently convicted of obtaining money by deception from the Halifax Building Society.

The investigation into the allegations made against Police Constable Munden was carried out by members of the Suffolk Constabulary, and the prosecution was undertaken by the Crown Prosecution Service for the Suffolk Area. In view of this I have forwarded your letter to the Deputy Chief Constable of the Suffolk Constabulary for his information and the information of the Crown Prosecution Service.

Any action taken against Police Constable Munden in relation to his conviction will be made under the Police (Discipline) Regulations 1985, which instruct all Chief Officers on breaches of the Discipline Code and the scope of punishments intended for such a breach.

Yours faithfully,

D. R. Winser A/Deputy Chief Constable

Re: Threatening E-mail (Hasker, RISKS-15.60)

Peter B Ladkin <pbl@compsci.stirling.ac.uk>
1 Mar 94 16:02:32 GMT (Tue)

Rob Hasker wrote in <u>RISKS-15.60</u>, concerning an E-mail threat to the life of the US President:

- > (Local news reports suggest that the student intended this to be a
- > practical joke. As I see it, the risk is in assuming that it doesn't
- > really matter what you say by e-mail.)

It may be premature to assign a RISK, since one doesn't yet know any motive. But there is a prima facie argument against Hasker's suggestion of prime RISK, which is that if it doesn't matter what's said in email, then one might as well send it in the clear. And Reincke didn't.

It seems that Reincke intended either (a) to confuse the audit trail, or (b) to give others the impression he was trying to confuse the audit trail. If (a), then it shows the risks involved in using a traceable fake; if (b), maybe he wanted to get caught and prosecuted (this is a known characteristic of some of those who engage in criminal activity of various sorts), and succeeded in doing exactly what he tried to do - in which case there seems to have been no computer-related RISK at all to him!

Peter Ladkin

✓ Bounties for Safety-Critical Software (Chastain, RISKS-15.60)

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
1 Mar 94 16:24:39 GMT (Tue)

- > Here's the [suggestion]: the government organization which is purchasing the
- > safety-critical software publishes the specification, the entire source
- > code as delivered by private contractors, and technical documentation
- > on the hardware environment. It then offers a bounty to any party
- > anywhere who demonstrates a logical error in the software.

Data exist (there's apparently a JPL study) to support the assertion that in safety-critical software, many more errors are usually to be found in the requirements specification itself than in the match between the delivered software/hardware and the requirements spec. If this is correct, information delivered to the public according to Chastain's suggestion would need to be supplemented by information enabling the requirements spec itself to be critiqued. Documentation on the hardware environment is unlikely to be sufficient by itself. I have only the usual numerous and incomplete suggestions as to what the extra needed info could be.

However, there are examples in which Chastain's suggestion, unsupplemented, could have helped. Consider the September 1993 A320 accident in Warsaw. Inspection of the requirements (in this case, simply the info contained in the Pilot's Operating Handbook) reveals the design that fatally inhibited deployment of the braking systems after the plane had landed.

Peter Ladkin



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 62

Thursday 3 *March* 1994

Contents

Joe Camel's 10,000,000 best friends

Phil Agre

Double Posting of Credit Card Charges

Bryan Apple

Video Tech & Privacy... what's becoming possible

David Honig

RISK of computer-controlled landings

Simson L. Garfinkel

Headline: "Child molesters use computer talk as bait"

David Tarabar

Conviction for spreading virus?

Laurel Kristick

'We {Will} Find you...'

Paul Robinson

Local TV News Report Misses The Boat

Dan Danknick

Educating on the RISKS of the Internet

Jeremy Epstein

Will they ever learn? [Passwords]

Roger Binns

One time Passwords and Encryption

A. Padgett Peterson

Of Locks and Legends

Dave Pierson

Impact fuel cutoff anecdote, risk

Bob Wise

NTIA Releases Notice of Inquiry on Privacy Issues

Beth Givens

SIGSOFT 94 Call For Papers

Dave Wile

Info on RISKS (comp.risks)

✓ Joe Camel's 10,000,000 best friends

Phil Agre <pagre@weber.ucsd.edu> Thu, 3 Mar 1994 09:03:13 -0800

The 3/3/94 New York Times includes a long, fascinating article on recent trends in cigarette advertising, away from mass media like billboards and magazines and toward database-oriented marketing based on promotions. The full reference is:

Allen R. Myerson, Selling cigarettes: Who needs ads?, New York Times, 3 March 1994, pages C1, C5 (business section).

Here are two paragraphs from the middle of the article:

... Philip Morris marketers boast that the Adventure Team promotion and a carefully calculated price cut restored Marlboro's share of the \$42 billion cigarette market from 22 percent last March to nearly 27 percent in January, widening its lead over all other brands. Flush with the names and addresses of their new customers, they are planning their next campaign.

Over at R. J. Reynolds, Philip Morris' major rival, marketers pride themselves on computerized data banks so huge and detailed that they can go far beyond merely aiming their discount coupons and Camel Cash merchandise offers at the less than one-quarter of Americans who smoke. They can choose not just smokers of competing brands, but those who smoke brands with price, taste and image most like those of Camels, for example. In fact, Reynolds can select from that last group just those smokers who would gladly switch, for a few pennies a pack, or perhaps an ashtray or cap.

These trends have the virtue that non-smokers get exposed to less cigarette advertising, thus lessening the force of claims that such advertising is recruits new smokers rather than getting existing smokers to switch brands. On the other hand, mass cigarette advertising (such as glossy booklets urging folks to "Get More Gear") is not going away; indeed it is an integral part of the new strategy. Finally, and most importantly for Risks, the cigarette companies' increasingly personalized connections to their customers may inhibit smokers' attempts to end their addictions, since they will now be exposed to ever-more-customized stimuli encouraging them, if only implicitly, to continue smoking. This is only speculation, of course, but it's an important test case for the social implications of data-intensive one-to-one marketing, and it should be watched closely.

Phil Agre, UCSD

Double Posting of Credit Card Charges

Bryan Apple

bha@offsite.com>

Wed, 2 Mar 94 13:12:36 CST

In a 16 Feb 1994 letter from The Chicago Symphony Orchestra, Henry Fogel, Exec. VP describes a "computer error". It seems that all American Express

charges for tickets and contributions since 1991 were re-submitted. Considering my seats cost nearly \$100 each, this could represent a significant amount of money. The letter does not identify which party (Amex or the CSO) caused the error.

The letter says, "Charges for these items will appear again on your next statement...", and continues, "In most cases, these charges will also be removed on the same statement."

The risks include:

Transaction systems that don't range check their input (shouldn't charge dates have to be somewhat current?).

Automated postings that aren't tied out to an independent check (Wow, sales were up 3,700% this month!).

Bryan Apple, Data Vault Systems (708) 885-6000

✓ Video Tech & Privacy... what's becoming possible

David Honig <honig@ruffles.ICS.UCI.EDU> Thu, 03 Mar 1994 12:43:00 -0800

In the Feb 94 "Advanced Imaging" magazine, there is a discussion of how video cameras (from above, preferably, for contrast and occlusion reasons) are being deployed with machine vision systems in malls. The stated purpose is to measure people flow, to learn about buyer behavior. Sort of like machine vision applications for traffic flow monitoring. There is mention of secondary sensors causing cameras and vision systems to "orient" [my interpretation] towards some situation.

In the same issue there's an unrelated advert for something called an "imputer" which is a white palm-sized box with a lens. (Looks like an aperture of about a cm.) Next to it is the circuit board presumably within the white box. It contains 4 chips: an imaging chip and a microcontroller among them. One of the chips is socketed. You can develop algorithms on your desktop machine and then load them onboard, it seems. And have your own standalone motion-interpretation system.

✓ RISK of computer-controlled landings

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Thu, 3 Mar 94 16:50:16 -0500

I was on one of the few aircraft to land in the Boston blizzard today. There was zero visibility. When we hit the runway (ouch!), the plane veered back and forth, slipping on the ice, apparently working differential thrust.

After we landed, the pilot said "in case anybody is interested, you are in one of the few Northwest Airbus 320's capable of landing itself, which it just

did."

And I thought, "oh, wow."

And I wondered which would have been RISKier: landing on autopilot, or landing on human pilot.

Headline: "Child molesters use computer talk as bait"

David Tarabar <dtarabar@hstbme.mit.edu> Thu, 3 Mar 83 08:53:02 -0500

This is the headline of article in the 3/3/94 Boston Globe on the front page of an inside Metro/Region section.

For most parents, the thought of their child sitting in a bedroom and skillfully using a computer is a source of comfort and pride"

Increasingly, however, the home computer has become a source of danger, as manipulative child molesters reach out to unsuspecting children through thousands of interactive and easy-to-use computer bulletin board systems."

... The news article triggering this discussion article is:

A 23-year-old Chelmsford [Mass] man pleaded not guilty to an attempted kidnapping charge after he allegedly used a computer bulletin board to attempt to coax a teen-ager into helping him abduct a young boy for sexual purposes

The article goes on to explain BBS systems and how they allow impersonal contact between juveniles and child molesters. Law enforcement officials in Massachusetts have been concentrating upon (and getting publicity) for investigating computer assisted child-abuse. There have been several other charges, and in 1992 a Cambridge man pleaded guilty to raping two boys who he met through a BBS.

[Also noted by Bob_Frankston@frankston.com. PGN]

Conviction for spreading virus?

Laurel Kristick <kristill@robie.cs.trw.com> Wed, 2 Mar 94 13:44:53 MST

In Amnesty International's Freedom Writers list for February 1993, one of the letters is to the Cuban Government on behalf of Luis Grave de Peralta Morrell and 3 other scientists. They were convicted in February 1992 of various charges and given sentences which varied from 8 to 13 years.

Evidence against them included a book written by Luis Grave de Peralta which criticized the Cuban Government. Earlier, he had lost his position as professor of physics at the University of Oriente after resigning from the

Cuban Communist Party.

One of the charges against them was "that the four had been trying to spread a computer virus." Amnesty International claims that no clear proof of this was offered during the trial. Does anyone have more details on this? What kind of virus were these individuals supposedly trying to spread?

The RISK? I suppose that if a totalitarian government is out to get you, they will use any possible charge against you, including computer-related ones.

Laurel Kristick kristill@robie.cs.trw.com

✓ 'We {Will} Find you...'

Paul Robinson <PAUL@TDR.COM> Wed, 2 Mar 1994 23:17:29 -0500 (EST)

In an article on the cover of the February 10, 1994 {Washington Technology} magazine of the same name, talks about a specialized use of biometrical information (specific details unique to a person like size, etc.) to identify them.

The idea behind this is that in an airport, an infrared camera is mounted near the arriving passengers section, taking pictures of every person who is passing through the facility. This captures the 'aura' or underlying facial vascular system (pattern of blood vessels and such). In 1/30 of one second, it captures the data and forwards it via high-speed data lines to an FBI database that has stored auras of the worlds most-wanted criminals and terrorists, then matches generate an order to nab a suspect, supposedly producing "a piece of evidence that is as rock-solid as any presented to a court."

Currently, infrared cameras are being attached to desktop computers to create digitized thermograms of people's faces in 1/30 of a second. The company that is working on this technology, Betae Corp, an Alexandria, VA government contractor, claims that the aura is unique for every single person. The photos in the front of the article show two clearly different thermographic images that are claimed to be from identical twins.

The facial print does not change over time (and would allegedly require very deep plastic surgery to change it), retains the same basic patterns regardless of the person's health, and can be captured without the person's participation. The technology will have to show it is a better choice than current biometric techniques such as retinagrams (eye photographs, voice prints and the digital fingerprint.

A Publicity-Shy Reston, VA company called Mikos holds the patent for certain technology uses of this concept. Dave Evans of Betac who has obtained certain "non exclusive" rights in the technology claims that "thermograms are the only technology he has seen in his more than two decades of security work that meet the five major criteria of an ideal identification system: They are unique for every individual, including identical twins; they identify individuals without

their knowing participation; they perform IDs on the fly; they are invulnerable to counterfeiting or disguises; they remain reliable no matter the subject's health or age," the article said. Only retinal photos are equivalent, but potential assassins aren't likely to cooperate in using them.

Right now it takes about 2-4K per thermograph, (it says '2-4K of computer memory' but I suspect they mean disk space) and that's not really a problem for a PC-Based system of 2000 or so people going to and from a building; it's another magnitude of hardware to handle millions of aircraft travelers in airports. Also, infrared cameras are not cheap, in the \$35,000 to \$70,000 range, which, for the moment is likely to keep small law enforcement facilities from thermographing all persons arrested the way all persons arrested are routinely fingerprinted. But we can expect the price to come down in the future.

The writer apparently had to agree with Evans not to raise privacy and security issues in the article, it says, since first they have to show the technology works. But even it raised questions:

- The technology could be a powerful weapon in a "big brother" arsenal, with cameras in front of many stores and street corners, scanning for criminals or anyone on the government's watch list?
- Does the government have the right to randomly photograph people for matching them against a criminal database?
- What guarantees do we have that thermographs are actually unique for every person, or that the system is foolproof?
- What is the potential for blackmail, with thermographs to prove people were in compromising places and positions?

There are also my own points.

- While this can be used to protect nuclear power plants against infiltration by terrorists (as one example it gives), what is to stop it, for example, to be used to find (and silence or eliminate) critics and dissidents? I wouldn't give China 30 seconds before it would use something like this to capture critics such as the victims of Tianamen Square.
- Long history indicates that better technology is not used to improve capture of criminals who violate the lives and property of other private parties, it is used to go after whatever group the government opposes. That's why people who defend themselves with guns against armed criminals in places where gun controls are in effect, can expect to be treated harsher than the criminal would have been. Existence of criminals supports the need for more police and more police-state laws; defending oneself against criminals shows the ineffectiveness of those laws.

Paul Robinson - Paul@TDR.COM

Local TV News Report Misses The Boat

Dan Danknick <ddanknic@cisoc.canon.com> Thu, 3 Mar 94 13:46:54 PST

Last night there was a news report on our local KABC affiliate about a man who had been arrested at a local bank for wandering around the parking lot in the area of the automatic teller machine and acting very suspiciously. Evidently a bank patron thought this odd and flagged down a passing police officer. In a search of the suspect's van that followed, a few hundred blank ATM cards were found as well as nearly \$5,000 in twenty dollar bills. The man had apparently been "shoulder surfing," the act of peering across the shoulder of an ATM client to garner their PIN number as it is entered. Such a surfer then acquires discarded transaction slips in the region of the ATM, matches the transaction time up with the acquired PIN, programmes a card, and with-draws a good chunk of money.

Yes, this is nothing new. But where the TV reporter had an excellent opportunity to remind viewers to _always keep your transaction receipt_ (throwing it away at home if you have to) they neglected to. Instead, I was presented with a number of interviews with patrons explaining the various methods they used to conceal their PIN entry actions (my favorite was a woman who explained that she could type it so fast, nobody could ever see it.)

Great. Another chance to bring the general public up to speed lost in poor journalism. Maybe all news services should have a RISKs reader on staff?

Dan Danknick ddanknic@cisoc.canon.com

Educating on the RISKS of the Internet

Jeremy Epstein -C2 PROJECT < jepstein@cordant.com> Wed, 2 Mar 94 10:21:11 EST

The RISKS of sending credit card numbers (and other such information) over the Internet are well known in this group, so I won't rehash it.

I recently received an inquiry from the organizer of an upcoming conference about the security ramifications of accepting electronic registration. They want people to upload (into their World Wide Web server) the registration data, including a credit card number. The data is then processed and the information (including the credit card number) is e-mailed to the registration agent. The person who made the inquiry had a suspicion that all of this electronic traffic might have some security implications, but wasn't sure.

The point of this note is that even though readers of *this* forum know the RISKS, as more and more people join the Internet we need to deal with education. If the Internet community doesn't warn people of the do's and don'ts, the Internet will get a black eye when the inevitable fraud occurs.

--Jeremy Epstein, Cordant, Inc. jepstein@cordant.com

One time Passwords and Encryption (Kabay, RISKS-15.61)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Thu, 3 Mar 94 21:15:53 -0500

IMHO passwords have been used since before the Roman empire and their effectiveness has only gotten worse - back then they were changed daily.

I have been using tokens for nearly five years now & a couple of years ago wondered (both publicly and in print) why, instead of using the token's output for authentication, it was not used as the seed for autoigniting encryption since both sides had the result and it had never passed on the line. Since most token's responses are seven bytes long, DES seemed to be a natural that was well documented.

The fact that you could communicate would authenticate both ends of the line and would be resistant to a "man-in-the-middle" attack. Talked to two vendors about it & both said "fine - you fund it and we'll do it".

The RISK is always that if you wait too long to develop a product, you will wind up getting Clipped.

Padgett

✓ Will they ever learn? [Passwords]

Roger Binns <rogerb@x.co.uk> Wed, 2 Mar 1994 10:27:28 GMT

The North Carolina State University has proudly announced their web server to the net on the NCSA What's new page. Having a look I spotted the following easy steps to compromising an account there ...

- : The username is generally composed of the initial letters of the user's
- : first and middle names and the first six characters of his or her last
- : name. For example, if the user's name is John Q. Public, then the username
- : would be japublic.

:

- : The password that users are given initially is their social security number,
- : which is typed in the password field without the dashes (e.g., 123-45-6789
- : is 123456789). In order to prevent unauthorized access, users need to change
- : their passwords as soon as possible and never share their passwords with
- : anyone.

I wonder how many illegal accesses they have?

The original is http://www.eos.ncsu.edu/eos access/accounts.html

Roger Binns, Software Engineer, IXI Ltd, Cambridge, UK rogerb@x.co.uk



Of Locks and Legends

<pierson@cimcad.enet.dec.com>
Thu, 3 Mar 94 14:00:21 PST

A recent RISKS reported on a "kick to enter" interaction in certain late model automobiles. The current Autoweek, quoting a manufacturer's press release calls this a "high-tech legend". Among other things, the air bag mechanism is deactivated within 150 milliseconds after the ignition is turned off. (I assume the delay is to allow for the ignition circuit "dropping" in an accident.)

dave pierson Digital Equipment Corporation pierson@msd26.enet.dec.com

[Also noted by eli@cisco.com and silas@Informatik.Uni-Bremen.DE (Stefan Mahnke). PGN]

Impact fuel cutoff anecdote, risk

Bob_Wise <rmwise@mcigate.apdev.cs.mci.com> Mon, 28 Feb 1994 21:20:46 -0700

This has been well-known dirty trick in showroom-stock autoracing (IMSA Firehawk and SCCA Showroom Stock, primarily) for many years. The impact sensor is typically in the rear of a car. A firm bumper-to-bumper tap from behind will often lead to an impact sensor shutting off the electric fuel pump, usually resulting in a DNF for the bumped driver. Many showroom-stock competitors bypass the impact cutoff to keep this from happening, thus leading to real risk in the case of a serious accident.

I find it strange that the airbag system in the early Ford airbag cars (as indicated in the post above) was triggered by a sensor that is typically found in the rear of the car.

Side note: road racing organizations such as IMSA and SCCA require the disabling of any airbag systems. The safety equipment required negates the use of passive systems.

-Bob Wise, #64 SCCA American Sedan Mustang

NTIA Releases Notice of Inquiry on Privacy Issues

"Beth Givens, Privacy Rights Clearinghouse" <B_GIVENS@USDCSV.ACUSD.EDU> Thu, 3 Mar 1994 17:43:33 -0800 (PST)

CONTACT: Larry Williams (202) 482-1551 MARCH 1, 1994

The National Telecommunications and Information Administration (NTIA) is

undertaking a comprehensive review of privacy issues relating to private sector use of telecommunications-related personal information associated with the National Information Infrastructure (NII).

Public comment is requested on issues relevant to such a review. After analyzing the comments, NTIA will issue a report and make recommendations as needed.

The inquiry will focus on potential uses of personal information generated by electronic communications, including interactive multimedia, cable television and telephony. NTIA is studying the issues that arise when such telecommunications- related information is used to create detailed dossiers about individuals. NTIA seeks to determine whether any overarching privacy principles can be developed that would apply to all firms in the telecommunications sector. In addition, NTIA is soliciting comment on other countries' actions to ensure the privacy of information transmitted over telecommunications networks, and to ascertain how any U.S. policies in this area will affect the international arena.

The Notice of Inquiry and Request for Comments appears in Part IX of the February 11, 1994, Federal Register and is also available on the NTIA Bulletin Board at (202) 482-1199. Set communications parameters to no parity, 8 data bits and 1 stop. Go into the menu "Teleview-Public Notices and Comments." File size is 48,514 bytes or about 18 pages of text. Internet users can telnet into the BBS at ntiabbs.ntia.doc.gov.

Comments should be filed on or before March 30, 1994. NTIA is accepting comments in writing or posted electronically via its BBS.

If you have further questions, please contact Carol E. Mattey or Lisa I. Leidig at the Office of Policy Analysis and Development, NTIA, 202-482-1880.

✓ SIGSOFT 94 Call For Papers

Dave Wile <wile@ISI.EDU> Wed, 02 Mar 94 16:48:45 PST

CALL FOR PAPERS
The Second ACM SIGSOFT Symposium on the
Foundations of Software Engineering
New Orleans, Louisiana USA
6-9 December 1994
Sponsored by ACM SIGSOFT

The ACM SIGSOFT '94 Symposium on the Foundations of Software Engineering will focus on innovative research results that identify and contribute to the foundations of software engineering. The intent is to help establish software engineering as a viable engineering discipline.

We solicit papers in all technical areas of software engineering. A successful paper is expected to report on new principles, methods, or results of experimentation in software engineering (which includes topics related to

the specification, design, implementation, and evaluation of software systems). Papers should emphasize how they contribute to a foundation that allows us to effectively engineer classes of complex software systems in disciplined, reasoned ways. Unless a strong tie to software engineering is made, papers more central to other aspects of computer science should be submitted to conferences in those areas.

A paper should clearly state the contribution and its underlying assumptions. It should also assess the results, making appropriate comparisons with and references to the literature. Papers will be judged on clarity, significance, relevance, correctness, and originality. The paper must contain ideas not previously presented in or currently waiting acceptance to another formal forum.

All papers will be reviewed by program committee members. In some cases, additional external advice may be solicited by the program committee. Papers of particular merit may be recommended to major software engineering journals for expedited review.

Submissions are limited to 12 pages (including figures) in 10 point type or larger, excluding references. Overly long submissions will be returned without review. Five copies, preferably double-sided, must be RECEIVED BY the program chair by MAY 31, 1994. Authors will be notified by AUGUST 5, 1994. Camera-ready versions of accepted papers are due, along with ACM copyright release forms, by SEPTEMBER 19, 1994. Proceedings will be distributed at the symposium and as a special issue of ACM Software Engineering Notes.

Tutorials will be held on Tuesday, DECEMBER 6, 1994.

General Chair
W. Richards Adrion
Department of Computer & Information Science
Univ. of Massachusetts, Amherst MA 01003
(413) 545-2742 adrion@cs.umass.edu

Program Chair
David Wile
University of Southern California / Information Sciences Institute
4676 Admiralty Way, Marina del Rey CA 90292
(310) 822-1511 wile@isi.edu

Tutorial Chair Debra Richardson, University of California, Irvine

Local Arrangements Chair

Johnette Hassell, Tulane University

Program Committee
Lori Clarke, University of Massachusetts, Amherst
Alan Dearle, University of Adelaide, Australia
John Gannon, University of Maryland
David Garlan, Carnegie Mellon University
Carlo Ghezzi, Polytechnic University, Milan, Italy
Gail Kaiser, Columbia University

Axel van Lamsweerde, University of Louvain, Belgium Mark Moriconi, Stanford Research Institute David Notkin, University of Washington Barbara Ryder, Rutgers University Dick Taylor, University of California, Irvine Ian Thomas, Consultant Walter Tichy, University of Karlsruhe, Germany Jeannette Wing, Carnegie Mellon University Stan Zdonik, Brown University



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 63

Monday 7 March 1994

Contents

Yet Another Mistaken Identity

Mike Zehr

Philadelphia 911 Crash

Steve Pielocik

Service a computer, go to jail

Kriss A. Hougland

Court Case casts doubt on cashpoint credibility

Brian Randell

<u>'Hacker' alters Drug Protocol in British Hospital</u>

Peter B Ladkin

Will Australia be doomed to repeat Clipper?

Rhys Weatherley

A Well Oiled Mac

Jon Golob

SCIENCE article critical of computer models

Jon Jacky

Re: Autopilot landings in `zero visibility'

Peter B Ladkin

The risks of user ID's

Jason Haines

RISKS RISKS: Bug in mailing RISKS-15.61

Mike Sullivan

PGN

Info on RISKS (comp.risks)

Yet Another Mistaken Identity

Mike Zehr <mikez@kenan.com> Mon, 7 Mar 94 08:21:02 EST

Boston Globe, Monday, March 7 -- (Summarized)

For the past 4.5 years, Clinton Rumrill 3rd has been trying to clear his name of financial and criminal problems caused by One of Rumrill's childhood

friends, John Mudge. Mudge apparently started by taking a department store credit card in Rumrill's name, has since racked up traffic charges, and been charged with ticket scalping, all in Rumrill's name and with Rumrill's social security number.

Although he's been able to clear up each case so far, because Rumrill and Mudge have very different appearances, new cases keep springing up. Rumrill has been told it would be easier to change his name and SS number than to keep trying to clear his name.

Rumrill now has another problem. Police have been made aware of the fact that Mudge is using Rumrill's ID, and now police computers think they are the same person!

The difficulties are made worse by the fact that in Massachusetts it is not a crime to give false information to the police.

-michael j zehr

Philadelphia 911 Crash

<spiel@aol.com>
Fri, 04 Mar 94 10:26:28 EST

KYW Radio reports that the 911 emergency service for almost the entire city of Philadelphia was out of service last night for several hours resulting in dozens of emergency calls not going through. Callers got a "try again later" message. The outage was reportedly due to a "software problem". Service has apparently been restored but the station reports that the authorities are still trying to correct the source of the problem. Nothing in the early edition of this mornings Inquirer but this sounds like a mini version of the ATT collapse of '90.......

Steve Pielocik Glenside, Pa. spiel@aol.com pielociks@smtpgate.nadc.navy.mil

Service a computer, go to jail

"Kriss A. Hougland" <hougland@enuxsa.eas.asu.edu> Thu, 3 Mar 1994 20:41:20 -0700 (MST)

I came across this report of a really nasty computer risk....

>From Electronics Now, April 1994, page 6 (I contacted the magazine to confirm this is NOT a joke and permission to post the article. Many thanks for Evelyn Rose, editorial assistant.)

NESDA Challenges U.S. Copyright Act

The National Electronics Service Dealers Association (NESDA) has come to the aid of Peak Computer Corporation in its legal battle with MAI Systems Inc.

NESDA and its associated organizations filed a friend-of-the-court brief

in Washington DC last November on behalf of Peak which has been sued by MAI Systems for alleged violations of the U.S. Copyright Act.

MAI says the software which operates its computers is licensed only to the owners of those computers, and only licensed owners should be allowed to turn them on. Its suit charges that Peak and other service companies are breaking the law by turning on the computer for service.

Two lower courts agreed with MAI that by turning on a computer a "copy" of the operating program is made in the computer's RAM. This, MAI says, violates Sec. 117 of the U.S. Copyright Act.

NESDA believes that if the ruling is allowed to stand, manufacturers of such products as appliances, audio and video equipment, and heating and air-conditioning controls could claim a similar exclusive right to their "intellectual property." According to NESDA Executive Director Clyde Nabors, "NESDA has no choice but to oppose" the lower court's ruling, which he views as "another of a long string of thinly-veiled attempts by some manufactures to eliminate competition from independent service [organizations]."

The NESDA brief challenges the ruling on several points of law. In its brief, NESDA referenced a previous Supreme Court ruling that concluded that a market for the service of a product exists after the sale of the product. In effect, the Court said that even if a manufacturer does not monopolize the sale of its product, it can still be charged with illegally trying to monopolize the service of those products.

The NESDA brief entitled the "Service Industry Signal," is being filed by attorney Ron Katz of the San Francisco office of Coudert Brothers, a New York law firm. To recover the cost of the brief as well as the cost of future "signals' from the service industry, NESDA has requested contributions to the "S.I.S" legal defense fund from concerned service dealers and technicians. The contributions are to be sent to the SIS Fund, c/o NESDA, 2708 West Berry Street, Fort Worth, TX 76109.

I am aware that some companies (Borland) have a "book" type of license. I would hate to have to bail out my car mechanic when the SPA busts him/her for turning on my car to try and fix it.

Court Case casts doubt on cashpoint credibility

Brian Randell <Brian.Randell@newcastle.ac.uk> Mon, 7 Mar 94 14:02:35 GMT

Court Case casts doubt on cashpoint credibility, by Mark Ward *Computing* (UK weekly), 3 Mar 1994

ATM's are in the news again after the Halifax Building society's court-rrom defence of their reputation.

Almost all high-street financial institutions are now facing a combined lawsuit brought by Denis Whalley of Liverpool solicitors, J Keith Park, on behalf of 66 clients who claim they have been victims of phantom withdrawals from automated teller machines. The case follows that of Suffolk policeman John Munden. He was convicted of attempting to obtain money by deception when he queried the Halifax over a series of transactions he claimed he had not

made but which appeared on his bank statement (Computing, 24 February). The Halifax - the UK's biggest building society - decided to prosecute. Curiously, though, when the trial was convened it was adjourned because the building society could not offer any expert testimony on its security procedures. The case came to court late last month and led to Munden's conviction. He is due to be sentenced in the next couple of weeks. During the trial, the somewhat ramshackle nature of the Halifax's security procedures came to light. The central personal identity number (PIN) validation application was first developed in 1978 and reworked in 1981, when the Diebold series of cash machines were bought. It doubtless it has been tweaked since, but it is still a system built for a less demanding era. Banks and building societies alike are trying to patch up the failing security procedures of their cash machines by putting in cameras and looking at other ways to prove users are who they claim they are. But the Halifax is not alone in trying to use old technology to meet changing customer needs. Every high-street bank and building society is closing branches or working out how to turn them into selling spaces rather than service points. And one man at least is convinced that this and other trends will make the cash machine a museum piece by 2010. A book, published next month, by author Bryan Clough, Cheating At Cards: Sharp Practice and Naive Systems, takes a long look at cashpoint crime. Clough believes the high pnce of ATMs in terms of pounds and pain could force a banking revolution. He says in many US states, so many people are mugged and murdered while using ATMs that state governments are forcing banks to fit safety devices that nearly double the cost of holes in the wall. And this is before any consideration is given to making the machines less fallible. The UK's first recorded incident of a person murdered after using a cash machine occurred in Hampshire this January. Clough is sure there have been others, though no one is collecting figures. He is convinced that retailers have an enormous opportunity to take business away from the banks, with the secure environment they offer people for getting cash when using debit cards to buy their shopping. That advantage is compounded by the fact that the cost to supermarkets of being able to offer the service is only that of a (pounds)50 swipe terminal and the connection to the bank's computer. Certainly, there is a real contradiction between banks and building societies trying to turn a branch into a space through which to sell more services, and their putting a machine on the outside that means customers have no contact with branch staff.

Regulatory bodies regard cash machine fraud as small beer. According to the Association for Payment and Clearing Services, the body that comments on security, ATM fraud in 1992 cost banks and building societies (pounds)3m, compared with the (pounds)165m cost of plastic card fraud. Apacs sees cash machines as a relatively secure method of dispensing money. Some are even looking at extending the PIN concept to plastic cards to cut the level of fraud at the point of sale. An Apacs spokesman said there are various studies being conducted that will result in technology to aid decisions at the point of sale. He said one problem lies in limiting false rejections - turning away genuine customers. He suggested a false rejection rate of one in 100,000 as acceptable. No technology on trial has yet demonstrated anything like this rate. What is clear is that crunch time is coming for the humble cash machine. Will it go the way of all flesh, or become the preferred method of dealing with your bank-only this time with the banks paying for their mistakes.

'Hacker' alters Drug Protocol in British Hospital

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
7 Mar 94 18:22:32 GMT (Mon)

In the German news magazine Der Spiegel 1994(9) 28/2/94 p243 is a story concerning Dominic Rymer, who obtained a doctor's password by looking over his shoulder, and then edited the drug protocol of a nine-year-old meningitis patient to something that might have killed her. This all happened at the Arrowe [sic] Park Hospital in Wirral, Lancs. I didn't see any article about it in a British newspaper.

Peter Ladkin

✓ Will Australia be doomed to repeat Clipper?

Rhys Weatherley <rhys@cs.uq.oz.au> 6 Mar 1994 08:55:07 GMT

I was looking through "The Sunday Mail" here in Brisbane, Australia on Sunday, March 6, when I noticed an article on page 20 titled "New Phone Stumps Oz Spy Group". I'll paraphrase it and give a few excerpts.

The key point was that the new digital Telecom Talkabout system which has been deployed here in Brisbane "cannot be traced or bugged using current technology". Talkabout is a "small cell" mobile phone system: there are now Talkabout poles all over the CBD and most suburbs, and people can buy a cheap small mobile phone to take advantage of the system. It is quite popular.

What the above quote probably means is that the police, ASIO (domestic security) and ASIS (Australia's CIA), don't currently have scanners that can decode the digital signals, although I suspect that Talkabout probably also uses the GSM encryption system which was introduced here recently, over the objections of the afore-mentioned agencies.

Of relevance to the Clipper debate is the following quote: "Telecom corporate public relations spokesman, Mr John Tucker, said it was a requirement of the federal Attorney General's department that all telecommunications be capable of being intercepted by intelligence and police agencies". Telecom have special dispensation from the Attorney General to run Talkabout as a trial as long as it is contained to the Brisbane network. The future of the system would be discussed after the trial and a decision would be made as to who would fund the cost of developing means of tracing calls.

So, it looks like Australia is doomed to repeat the same battle for strong encryption that is currently raging in the United States.

The usual RISKs of "buggable" encryption systems apply, but an additional RISK for Australia is that the Attorney General will buy the US government's line on Clipper and put our telecommunications at risk with all of the keys stored in databases held by a foreign power, no matter how friendly that power may currently be. Either that or the Attorney General will commission

the development of a similar system here. Another RISK is that once a tracing mechanism is developed, the "small cell" nature of Talkabout might permit the tracking of a user's every move.

The cynical members of the Clipper debate will put this down as yet another power that the US government seeks over its citizens and the rest of the world. The NSA for one would have no restrictions against monitoring the Clipper-ised internal communications of another country: that is part of their purpose for existence.

Probably the only good sign is that since Talkabout is very popular (and Telecom have been pushing it very aggressively), Telecom will probably fight tooth and nail to keep their investment, and the concerns of the above agencies will be overridden. The agencies will then be forced to recognise that wiretap surveillance is coming to the end of its useful life whether they like it or not, and they will have to develop alternative means. We can only hope.

Rhys Weatherley, University of Queensland, Australia rhys@cs.uq.oz.au

A Well Oiled Mac

<jongolob@aol.com> Sat, 05 Mar 94 16:04:53 EST

Lurking in a computer lab in a High School is a Macintosh, a Macintosh that wasn't well oiled, a Macintosh that ended its existence abruptly during a High School music class. It was a Macintosh SE and like its many other brothers in the lab it had a little hole in the back of it in which oil was placed. The brilliant administrators at the school found out that when a computer is left on 24 hours a day, seven days a week and 365 days a year for seven years a computer gets worn out. An unsuspecting student sat down at his table, flipped on his keyboard and turned on his Macintosh SE like he always did. The Mac slowly came to life, he clicked on the MIDI program and all hell broke loose. At first it started rather benignly, a gentle tap but, far worse things were about to come. Soon the Macintosh was going BUMP BUMP BUMP and was jumping on the desk. The student yelled for his teacher and the teacher proceeded to click on the mouse in a vain effort to fix the ailing computer. Next the Mac began to emit a grinding noise not unlike a garbage disposal.

The teacher screamed "DID YOU OIL IT!!!!."

The student replies "YES I DID, YES I DID."

The Macintosh is now rapidly convulsing on the table. The screen began to flash black and white. Next the Mac started to emit a high pitched whine. All of the other students began to flee from the room, several female students began to cry and the Mac, like an animal slowly dying of blood-loss, began to spurt oil out of the little hole on the back of the computer coating several other computers. There is a gigantic BANG as the student runs for his life out of the room and pieces of glass slide out into the hallway. The moral of the story.... KEEP YOUR MACINTOSH WELL OILED.

Jon Golob s97jgol1@cranbrook.edu (after March 30) jongolob@aol.com

SCIENCE article critical of computer models

Jon Jacky <jon@violin1.radonc.washington.edu> Mon, 7 Mar 1994 10:04:55 -0800

RISKS readers may be interested in:

"Verification, Validation and Confirmation of Numerical Models in the Earth Sciences" by Naomi Oreskes, Kristin Shrader-Frechette and Kenneth Belitz, SCIENCE 263, 4 Feb 1994, 641 -- 646.

This article is a critique of computer modelling applied to such public policy issues as global warming and nuclear waste disposal.

>From the abstract:

"Verification and validation of numerical models of natural systems is impossible ... The primary value of models is heuristic."

The article struck me as a philosophical essay on the limits of modelling in general, rather than as a critique of particular models.

These authors do not use the term "verification" with its usual meaning in computing, rather they use "verified" to mean "makes predictions consistent with observations." In fact, the article does not consider computing issues specifically. I think a better title would have been just, "Validation and Confirmation ..."

- Jon Jacky, jon@radonc.washington.edu University of Washington, Seattle

Re: Autopilot landings in `zero visibility'

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk> 4 Mar 94 13:34:51 GMT (Fri)

In RISKS-15.62, Simson Garfinkel says:

- > I was on one of the few aircraft to land in the Boston blizzard today. There > was zero visibility. [...]
- > And I wondered which would have been RISKier: landing on autopilot, or landing
- > on human pilot.

It's well to wonder, but in this case there might not have been the option. There are three categories of Instrument Landing System (ILS) approaches, Cat I, II and III, and Cat III is further subdivided into A, B, and C. The categories are differentiated according to the minimum weather conditions required for landing. An ILS is, abstractly, a couple of radio homing beams. One, the 'localiser', beams down the centerline of the runway, so you can tell if you're left or right of it, and another beams up at an angle, usually between 3-5 degrees, from the touchdown point - the 'glide slope'. You or your favorite autopilot are supposed to follow the beams from 5-15 miles out. In order to land legally for most Cat I Instrument Landing System approaches,

besides the usual visibility conditions, some part of the runway, its lighting or its environment must be visible when you're roughly 200 feet above the ground (and therefore a few more hundred feet from touchdown). Cat II 'minimums' are lower, Cat III lower still. Furthermore, for air carriers, operation is only permitted with certain values of 'Runway Visual Range'. Special crew and aircraft certification is required for Cat II and III, and certain modes of operation are mandatory. It is possible that the landing described was made under Cat IIIA, in which case use of some automated systems is mandatory, and hand-flying is not an option.

A further question is: what form of safety analysis has been done to ensure that the requirement to use automated landing systems rather than people is appropriate for Cat III landings? Perhaps those RISKS readers who have extensive dealings with the regulatory authorities and the airplane manufacturers could tell us?

Peter Ladkin

The risks of user ID's

Jason Haines <jhaines@compsol.fidonet.org> Fri, 04 Mar 1994 16:04:01 +1100

At the end of each semester, my university publishes unit results by printing out the student number of each pupil and their unit scores. These results are then posted in a public area in the university. Since only the student ID number (and not the person's name) is printed, it is impossible to find out someone else's results unless you know their student ID number.

This was reasonable secure, as it was fairly difficult to find out someone else's student ID number without obtaining their student card. Unfortunately, the computing unit at the university have introduced a new scheme for allocating usernames to students. The username is comprised of the first letter of the user's surname, and the user's student ID number.

It is fairly easy to obtain someone else's username. They may give it to you for e-mail purposes. Their username will often appear in a window title on their physical terminal, or in their command prompt. Tools like 'who' could also assist in finding out another person's username without their permission. The inclusion of the first letter of the person's surname into the username makes such investigation even easier.

Thus, with only a small effort, any student with a computer account could quite easily obtain the student number, and then the results, of any other student who uses the system.

Of course the university may change it's policy on posting results in a public place, but somehow I doubt it.

RISKS RISKS: Bug in mailing RISKS-15.61

Mike Sullivan <74160.1134@CompuServe.COM> 04 Mar 94 22:51:25 EST

I was surprised to discover that <u>RISKS-15.61</u> arrived in my emailbox with a list of well over 100 "Apparently-to: user@domain" headers that appear to be a substantial portion of the mailing list.

★ Re: Bug in mailing RISKS-15.61

<Risks-Request@csl.sri.com> 07 Mar 94 19:59:23 PST

In an effort to avoid the problem of MCImail RISKS recipients getting each issue with the entire list of MCImail users on their sublist, for RISKS-15.61 I tried BCC on a sublist that at that time also included MCImail, CompuServe, NetCom, and a few other so-called services.

CompuServe gets added to the MORON list of services apparently unable to handle BCC, because they turned that into the long list of addresses that apparently worked just fine when sent TO the sublist. NetCom reportedly also got wedged as a result of my attempt to use BCC.

I GUESS YOU CAN CONCLUDE THAT BCC: MAY BE VERY RISKY!

In <u>RISKS-15.62</u> I solved that problem by creating a BCC sublist just for MCImail and reverting to TO for everyone else on the rest of that sublist. I feel like a three-TO:ed sloth. But the degenerative "services" are really causing me too much grief. (I presume you recall the fact that several of them bounce the entire list if one address fails.)

GROAN. PGN



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 64

Thursday 10 March 1994

Contents

Irony & embarrassment

Gene Spafford

Another twist on Harding e-mail breach

John C. Rivard

Maybe appalling grammar is bad language design

Don Norman

Wrong credit card in the mail

Stephanie Leif Aha

Troubled water crossing bridge

Harald Hanche-Olsen

Calling-Number-ID catches obscene caller

Richard R Urena

X windows makes patient breathless

Govinda Rajan and Mathew Lodge

Trouble in comicland?

Arthur Goldstein

Getting help on the Internet

Phil Agre

Re: Clipper

Keith Henson

Carl Ellison

Stanton McCandlish

COMPUTER RISK! [Early April Fooling?]

Simon Travaglia

Info on RISKS (comp.risks)

Irony & embarrassment

Gene Spafford <spaf@cs.purdue.edu> Tue, 08 Mar 94 20:15:54 -0500

Twice in the last 6 months I have received a rather interesting brochure in the mail. Before I comment on it, let me describe it.

The first page is bright yellow, with the picture of a small guinea pig. In big letters, it proclaims "Microsoft would like to use your company as a test site for the 4,000,000 lines of new code in NT."

Inside, it states "SunSoft would like to offer you a leading-edge operating system with 10 years of fine-tuning behind it: Solaris." It then goes on with other "ad-speak".

I find this amusing in several respects:

- It plays on a long-standing perception of many computer users that Microsoft does a poor job of testing their code (I am enclosing a humorous posting that circulated on the Usenet recently that also points this out);
- 2) It underscores one of the major, major concerns about using large software artifacts (e.g., NT) -- they are often poorly tested, and the consumer is usually the one to suffer;
- 3) Sun's Solaris has been the subject of several very public, very significant bugs and security lapses over the past several years. It is hardly something to crow about in comparison to NY.

When the first round of these ads came out a few months back, a great many of the engineers inside Sun were very chagrined by it. Several were even angry -- they got a lot of comment from people outside Sun struggling with bugs in tar, sendmail, lpr and other utilities. It makes Sun appear to be unaware and uncaring about existing bugs and problems.

Now, for a second round of mailing to appear is almost the height of cluelessness by the advertising folks.

Risks?

- 1) Advertising folks who don't talk to the software engineers or customer support people.
- 2) Companies that spend more money and effort getting problems out the door than they do on design and testing.
- 3) Using your company as the test site for 4 million lines of Windows NT. Or X million lines of Solaris.
- 4) If you develop a reputation for poor testing and poor customer service, it can be used against you in advertising.

[Spaf also included an item on People for the Ethical Treatment of Software (PETS). Because that item has already been widely circulated on the net, I have removed it here. But if you did not see it, you might ask spaf for a copy. PGN]

Another twist on Harding e-mail breach

John C. Rivard <jcr@msen.com> Thu, 10 Mar 1994 11:44:47 -0500

In the March 9-15 1994 issue (Vol XIV, No. 23 p.9) of the Metro Times, the freely distributed alternative newspaper in Detroit, Dennis Rosenblum reports on yet another ethically-questionable activity ironically associated with the

violation of Tonya Harding's e-mail at the Olympics. <"E-Mail blunder at Olympics" RISKS 15-58>

Both the Detroit News and the Detroit Free Press reported that Free Press sports reporter Michelle Kaufman--with two other reporters from other papers--broke into Harding's account, but did not read any mail. The Free Press story was printed on page 8D in the sports section, but the News printed its story on page 1A, the front page, and portrayed it as much more scandalous.

The News and Free Press operate under a Joint Operating Agreement (JOA), a controversial arrangement which allowed the two supposedly editorially independent papers to combine their business and production facilities to cut costs, with a 100-year federal antitrust exemption. Both papers argued successfully in federal court that the Free Press would go out of business if not for this agreement.

The twist comes in when the Detroit News ran a photo of Kaufman with their front-page story. The digital image was stolen from the production facilities in the News building, which both papers share. According to Rosenblum:

"It turns out that a photo of Kaufman which the News ran with its story came from Free Press computer files. A News editor had a composting room worker sneak along a copy of the digital photo file, without the knowledge of the Free Press."

"Ed Wendover, a leader of Citizens for an Independent Press, which opposed the JOA in court, considered it predictable. 'This is perhaps only a precursor of what happens when they move in together,' said Wendover, a suburban publisher."

"In a memo to editors at the News, Editor and Publisher Robert Giles termed it a 'clear breach of the security that is critical to maintaining editorial separation and independence...as required by the joint operating agreement."

The irony of this story is obvious, but the RISK involves the impact of lax computer security on the First Amendment issues concerning the distinct editorial voices that were promised under the JOA.

(Quoted with permission of the author.)

John C. Rivard, JCR Design and Consulting jcr@msen.com

Maybe appalling grammar is bad language design

Don Norman <dnorman@apple.com> Mon, 28 Feb 1994 18:41:14 -0800

A recent flurry of articles in RISKS talks about poor spelling and punctuation, including the common problem of confusing "it's" and "its". Let me try the argument that these errors, like so many so-called "human errors" are in actuality design errors -- language design.

English is well known for its peculiarities in spelling, in part due to its multiple origins that give rise to words with different historical roots, in part because so many reformers have tinkered with it, sometimes successfully, sometimes not (Ben Johnson, George Bernard Shaw and Noah Webster come to mind, and I am sure that RISKS readers can name others). As a result, the spelling is so inconsistent on the surface that it takes a Halle & Chomsky to write a learned book explaining that there is an underlying deep consistency. If it takes a complex book to explain it, then maybe spelling isn't "designed" with the user in mind.

Now take punctuation. One problem is that English uses the symbol ' for at least two separate meanings (not counting its use in quotations): contraction and possession, as in "that's my dog's ball." With words that are homonyms, so the same spelling indicates contraction and possession, the rule is that contraction wins use of the '. Hence, "It's not its fault," where "it's" is a contraction and "its" is a possessive.

Try explaining that to a non-native speaker of English. Hell, try explaining that to a native speaker.

If English weren't so stingy with symbols and used different symbols for possession and contraction, then we wouldn't have any problem. English doesn't use symbols to mark parts of speech such as subject, or indirect object (or, in a case-based framework, agent or recipient): why use a symbol to mark possession?

Anyway, some human error in spelling and punctuation is really a system or design error: blame evolution -- or those early typographers who transformed the spoken language into its printed form.

Don Norman, Apple Computer, Inc. MS 301-3UE, 1 Infinite Loop, Cupertino, CA 95014 USA dnorman@apple.com +1 408 862-5515 Fax: +1 408 255-7045

Wrong credit card in the mail

Stephanie Leif Aha <steph@ics.uci.edu> Tue, 08 Mar 1994 10:30:38 -0800

I just received my new credit card in the mail, only it wasn't mine. The paper enfolding the card had my name and account number but the card had a different name and account number.

The credit card company claimed that this had _never_ happed before, blocked both accounts as having lost/stolen cards and is sending me a new card.

I was really surprised to be the first one having this problem. I would assume that this could happen if the entire run of cards mailed was off by one and we all received the right paper with the wrong cards.

Compounding the problem, they have redesigned the card this year so that the names are printed in the same color as the card, making them hard to read.

Only by chance did I look closely enough to notice that it wasn't my card. Perhaps the entire line did go astray after all.

Stephanie Aha grad student ICS Dept. U.C. Irvine

Troubled water crossing bridge

Harald Hanche-Olsen <hanche@imf.unit.no> Tue, 8 Mar 1994 17:29:06 +0100

No computer risks in this one, but a nice example of an unexpected failure mode: When a water mains broke in downtown Trondheim yesterday, a basement was flooded. No big surprise, except the basement was across the river! The drains were all plugged with ice and snow, so the water ran across the nearby bridge.

- Harald Hanche-Olsen <hanche@imf.unit.no>
 Dept of Mathematical Sciences, The Norwegian Institute of Technology

Calling-Number-ID catches obscene caller

Richard R Urena <urena@miser.umass.edu> Tue, 08 Mar 1994 10:48:00 -0500 (EST)

An article by the Associated Press notes that a woman in Pembroke, Massachusetts, used the CNID feature to track down an obscene caller who had been bothering her since 1991.

After years of harassment, the woman signed up with her phone company for the CNID service, compiled a map with the numbers and addresses of public phone booths in her vicinity, and obtained a second telephone line to alert police.

Her efforts paid off last Saturday at about 2:30 AM, leading to the arrest of a 28 year old suspect, who was still on the phone when the police arrived.

X windows makes patient breathless

<lodge@ferndown.ate.slb.com>
Tue, 8 Mar 94 13:51:32 GMT

The following article was posted to the USENET newsgroup comp.os.lynx today. The group deals with a UNIX-style hard real-time operating system called LynxOS. LynxOS' primary market is the real-time process control market (which is also often a safety critical market).

I should explain that LynxOS threads are light-weight processes.

- > From: govinda@anest.fgg.eur.nl (N Govinda Rajan)
- > Newsgroups: comp.os.lynx

- > Subject: Window move in X holds up other threads even of higher priority
- > Date: Tue, 8 Mar 1994 10:43:50 GMT
- > Organization: Dept Of Anesthesiology, Erasmus University, Rotterdam
- > Message-ID: <govinda.48.2D7C56E6@anest.fgg.eur.nl>

>

- > When I move a window or resize a window, all other threads in any process
- > which has the X Main Loop [are] held up. For example, I have a process which
- > has the X Main Loop which starts a thread. This priority of this thread is
- > made higher than the process and it starts a count down timer and waits for
- > the timer signal, which is SIGALRM. When the timer counts down it does some
- > work (actually sends an analog signal through D/A convertor to an external
- > instrument) and restarts the count down timer once more and sigwaits once
- > more and so on. SIGALRM is supposed to be thread unique.
- > All goes well, except when I move a window or resize, then the timer thread
- > does not respond at all and as long as I have the mouse button pressed down
- > it does not respond. When I release it everything continues normally again.

So far, so good. The problem can be explained by the fact that when an X window manager wants to move or re-size a window, it "grabs" the X server to prevent other X events from interfering with the window move.

Now the comes the RISKy bit:

- > My external instrument is an artificial ventilator and if it does not get
- > the signal in time the patient does not get any breaths.

[temporary technical solution from article deleted]

So the patient's life depends entirely the timely delivery of a software signal (and nothing else)? The complete absence of any recognition that this is a safety critical system that could kill people horrifies me.

I think I'll be staying away from Dutch ventilators if at all possible...

Mathew Lodge, Software Engineer, Schlumberger Technologies, Ferndown, Dorset, UK, BH21 7PP lodge@ferndown.ate.slb.com (+44) (0)202 893535 x276

Trouble in comicland?

Arthur Goldstein <goldsten@cs.uiuc.edu> Tue, 8 Mar 1994 03:40:30 GMT

>From the March 7th, 1994 Blondie comic strip (without permission):

Dagwood Bumstead speaking and looking at bills:

"I don't get it! Why can't we keep up with all our bills?"

"We don't live high! We don't splurge!"

"Yet somebody keeps sending me all these bills!"

"Could they have me mixed up with some other Dagwood Bumstead?"

Perhaps Dagwood should check out comp.risks for other cases of duplicate identities.

Arthur Goldstein, Comp. Sci. Univ of IL, 1304 W. Springfield, Urbana, IL 61801 goldsten@uiuc.edu UUCP: {uunet,harvard}!uiucdcs!goldsten

Getting help on the Internet (Yurman, RISKS-15.57)

Phil Agre <pagre@weber.ucsd.edu> Sat, 5 Mar 1994 16:37:30 -0800

In response to Dan Yurman's note in <u>RISKS-15.57</u> about misguided teachers instructing students to send basic questions to Internet discussion groups, I've written a short article about how to ask people for information (on or off the net). The skills it describes are common sense to long-time net dwellers, but they're definitely not common sense to beginners. To fetch a copy, send a message that looks like:

To: rre-request@weber.ucsd.edu Subject: archive send getting-help

Feel free to post it to any discussion groups that have had this problem, or send it to teachers or students involved in courses that involve Internet-based research.

Phil Agre, UCSD

✓ Re: Clipper

<a href="mailto: <a href="mailto:
<a href="mailto:
<

If I may boil down the government's side of the Clipper debate, it is this:

"We need to implement this encryption method so as to avoid problems we think may be coming. Trust us! We promise not to abuse your privacy." Except, of course, Clipper technology gives them a 'pen register' on every phone. Pen register give those in power a running list of every phone contact made between two Clipper phones without the need to fill out even the minor paperwork now required for this surveillance.

I do not doubt the sincerity of Dorothy Denning or others who defend Clipper. And I would have fewer problems with Clipper/Capstone proposal if the people who will be granting access to the keys and those with legal access to the keys and call records were of Dorothy's caliber.

However, people of good will are not likely to be the ones who apply for these keys to your privacy in the future. I am right in the middle of a case which has remarkable similarities to a Clipper "request for keys."

Full details have been posted to comp.eff.talk and misc.legal, but in brief summary, a Postal Inspector from Tennessee is attempting (for political reasons) to impose the obscenity standards of that region on an adult BBS run from Milpitas (just North of San Jose). To this end, he obtained a warrant to take the BBS hardware. Because of contained email and First Amendment activities of a BBS, subpoenas, not warrants, are required under *two* sections of federal law. The laws are Title 42, Section 2000aa, and Title 18 Section 2701, the same ones which were applied in the well-known Steve Jackson Games case.

Pointers to these federal laws were *posted* on the BBS. The postal inspector downloaded this file and *included* it in his affidavit for a search warrant to a Magistrate-Judge in San Francisco, along with a remarkably weak theory of how he could avoid application of these laws to himself.

To obtain a warrant to take email and 2000aa materials, the laws require a number of judicial findings to be made. None of these requirements were considered by the court. The postal inspector got his warrant, mailed child pornography to the BBS, served the warrant, "found" the child porn and obtained an indictment in TN. The child porn charge is bogus because the agent specifically described the material as "sent without his knowledge" (referring to the sysop). Of course the sysop has to defend himself from the charges 2000 miles from home and shut down his business while doing so, and everyone on the system had their email copied and passwords compromised.

This example applies directly to the Clipper situation.

The risk under Clipper is that your private communications will be protected by the *weakest* link in the chain--one of the thousands of low level Magistrate-Judges among whom corrupt or zealous law enforcement agents shop for warrants and will shop for keys. These magistrates (who are *not* judges, but work for the US Attorney's office) tend to be busy, or lazy or corrupt or all three. As in this case, even if the law is *directly quoted* in search warrant affidavits or key requests, and these laws *expressly forbid* granting warrants or key requests under the conditions cited, the magistrate may not even read the supporting affidavit before approving it. He is *very* unlikely to read or consider the underlying laws when granting a request. The key escrow agents provide no protection whatsoever since they simply fill orders from agents with approved applications.

Judges ignore the law with impunity, and so do law enforcement agents because one agency will almost never investigate another.

As a practical matter, applications for search warrants are almost never denied. The same situation is certain to occur for Clipper key applications, no mater how weak the justification happens to be, or what laws are being violated by those seeking the keys.

Keith Henson

✓ re: Bidzos on Clipper (RISKS-15.61)

Carl Ellison <cme@sw.stratus.com> Tue, 8 Mar 1994 13:59:03 -0500

Jim Bidzos submitted his reaction to the Clipper proposal. I agree with him for the most part, but would add a few notes:

[risks of Clipper]

>- Potential abuses by government and loss of privacy for all citizens.

I would add:

increased vulnerability to Organized Crime (because they're not very experienced with cryptanalysis but they have lots of experience with bribery, breaking/entering, theft of machines and data, ... -- in other words, all the talents you need to break the key escrow scheme).

>AN ALTERNATIVE PROPOSAL

>

>One approach would be to have NIST develop a standard with three >levels. The first level could specify the use of public-key for key >management and signatures without any key escrow. There could be a >"Level II" compliance that adds government key escrow to message >preparation.

What's wrong with just having the FBI, NSA, GCHQ, French bureau (whatever it's name), ..., publish their own RSA keys (both PGP and RIPEM format) so that individuals can voluntarily include those keys as recipients when they encrypt, if they want to volunteer to give the gov't access?

This achieves exactly the voluntary wiretapping the NSA says it wants -- with no hardware and no special code.

>II products would be decontrolled for export. The market can decide; >vendors will do what their customers tell them to. This satisfies >the obvious desire on the part of the government to influence what >happens, as a consumer.

I disagree with any plan to control exportability based on the NSA's ability to read traffic. I believe nothing which is already available outside the US should be restricted from export. Anything else just makes the US government look stupid.

EFF's Barlow v. Denning on Clipper - AOL March 10, 9PM EST LIVE

Stanton McCandlish <mech@eff.org> Tue, 8 Mar 1994 20:07:02 -0500 (EST)

[Cc:ed to a lot of groups]

CLIPPER CHIP DEBATE

Thursday, March 10, 9 pm eastern

Dorothy Denning, cryptologist and chair of the computer science department at Georgetown University, will debate John Perry Barlow, cognitive dissident and co-founder of the Electronic Frontier Foundation, in the TIME Odeon on America Online this Thursday at 9 pm. Philip Elmer-DeWitt, TIME senior writer, and Robert Pondiscio, TIME public affairs director, will moderate. The floor will be open to questions from the audience.

You need an America Online account to participate. Call America Online at 703-448-8700 to subscribe.

Philip Elmer-DeWitt ped@panix.com ped@well.com TIME Magazine philiped@aol.com

✓ COMPUTER RISK! [Early April Fooling?]

Simon Travaglia <SPT@waikato.ac.nz> Wed, 9 Mar 94 15:34 +1300

Warning Notice M.U.D-1

On the 3rd of September, 1992 the computing world was rocked by the horror of a new computer-originated illness and the life it claimed.

Eldred Squires, a 26 year old Operator/Administrator at major British Chemical Company was the first victim. At approximately 9:03am, Squires logged into his personal account, ees, and sent some email to a friend at a remote site. Logging out, he then proceeded to log into the operator account to clean up some problematic printing queues. Following this, he logged out and logged into a test account to check that his print queues were accepting data from normal users. Finding that all was well, he logged out then logged into the root account to create a new username to receive helpdesk mail, not realising the mortal danger he was in. Wanting to test this new username, he logged out from root and proceeded to login to his new account. Barely three letters into his twelve letter alphanumeric password, he slumped forward across his keyboard, dead.

Investigators, on arriving at the scene could find no reason for his death and elected to wait for further information from the outcome of the Autopsy.

The Autopsy revealed that the victim's cerebral cortex suffered damage consistent with heating of the brain to approximately 120 degrees celsius. Still no nearer to the solution of the death, Computer and Workplace Safety Officers decided to recreate, using accounting logs and user audits, the circumstances leading up to the tragedy. Shielding the testing officer from the equipment with leaded glass, the team commenced their tests. Within five

minutes, another victim lay sprawled across the keyboard, a fine patina of sweat on their brow.

Admitting defeat, the Safety Office called in an expert in Computer Related Deaths, Dr Brian Analpeeper. Within minutes of examining the logs and audits Analpeeper was able to correctly diagnose the cause of death. Multiple Username Disorders.

Multiple Username Disorders, Analpeeper explained, are a dangerous new side-effect of the current computing mindset. People become encumbered with several usernames until, ultimately, their brain fries out. Analpeeper also explained that for years the Social Sciences had been aware of the existence of Multiple Personality Disorders (commonly mis-referred to as Split Personalities) and that in a small way, M.U.Ds were in fact a computer replication of this.

"People are required to maintain several accounts for various purposes, One for say, an Administration function, One for their own personal use, Another for normal work, and perhaps yet another for financial and charging matters. Sooner or later the combination of what is required of the user of these accounts will wreak it's havoc on the brain, causing mass cerebric hysteria. Of course some people have a higher tolerance to this than others, yet there is *no* way of accurately judging how far we can push a user."

Later, in a harmless demonstration, Dr Analpeeper, took a volunteer and assigned him 5 usernames for different purposes. Victim number 3 fell to the floor in a lifeless heap.

"I lied about it being harmless" Analpeeper said. "So sue me."

Months later scientists are still no nearer finding a solution to the problem, mainly because they're to scared to login to the research computers. Life goes on, or sometimes it doesn't.

Are you in danger?

In an effort to reduce the deaths and crippling side effects of Multiple Username Disorder, the Computer Risk Committee has compiled this list of warning symptoms:

Victim may:

- Wonder whether they've read their mail today
- Wonder which account they're logged into
- Complain of feeling hot and bothered in front of their terminal
- Complain that the room appears to be getting warmer
- Slur words, especially after consuming large quantities of alcohol
- Repeatedly forget passwords
- Ask to see the wine list at restaurants for no apparent reason
- Pause for a few seconds before entering their password.
- Talk to themselves whilst logging in or executing everyday commands.
- Fail to notice everyday events, such as telephones ringing, power failures, being struck about the head etc

- Fall to the floor dead.

Should one or more of these symptoms be present, STOP USING YOUR ACCOUNT NOW! Logout and walk away. Life is, after all, too precious..

Simon Travaglia, spt@waikato.ac.nz University of Waikato Computer Centre Hamilton, New Zealand +64-7-8562889 Ext 8347, FAX 838-4066



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 65

Friday 11 March 1994

Contents

Using Caller ID to catch obscene callers

anonymous

Hard-drive headache

Robert Telka

Digital Detritus

Eric Sosman

Stephen D Crocker

Re: Maybe appalling grammar is bad language design

Mark Jackson

Alayne McGregor

RISK to freedom of information

Philip Overy

Re: Clipper

Mark Eckenwiler

Daniel B. Dobkin

13th Intrusion-Detection Workshop

Teresa Lunt

First announcement of COMPASS '94, program and info

Teresa Lunt

Info on RISKS (comp.risks)

Using Caller ID to catch obscene callers

<[an anonymous contributor]> Thu, 10 Mar 94 xx:yy:zz xxT

The recently reported case of the woman using caller ID to catch an obscene caller was noteworthy only because of its relative rarity. Fewer and fewer such callers are stupid enough these days to make such calls from other than payphones, and most won't hang around the phone long enough to get caught. To the extent that an idiot does stay around, use of the call-trace feature that is an integral part of the new systems (which provides the number instantly to the telco, rather than to the callee) would provide the same info in a much less invasive manner.

The telcos know full well (all you have to do is read their own literature) that the real reason they push caller ID is to provide businesses with tools for phone number collection of inbound callers for building of telemarketing lists. Its overall usefulness for dealing with harassing calls is quite limited, and becoming less so every day as more and more of the callers catch on.

Hard-drive headache!

Robert Telka <watpod13@ccs.carleton.ca> Thu, 10 Mar 94 16:03:42 EST

Lisa Balkes' story of the Janitor interrupting the UPS brought back to mind a problem which I ran into this past summer. I will keep the company anonymous to protect it's identity. I was employed there during the summer as a student programmer/analyst. On with the story!

A new alarm system was being installed at company P over one weekend. The installers had to access the climate controlled computer room where company P's Prime system was located to incorporate the thermometer with the alarm system (if the air conditioner conks out, and the room gets too warm, the alarm is set off).

The installers were let into the room by the plant manager who was working that week, however there is an unwritten rule that only authorized personnel are to enter the room, and any unauthorized people are to be escorted.

When we arrived Monday morning, two of our three hard drives in the drive cabinet where crashed. We also noticed that the cabinet had been physically moved a few centimetres (there was an imprint of its original position left on the floor). The security alarm installers insisted that they did not move the units, yet they must have since they were the only people to enter the locked room that weekend. Since nobody saw them do it, we had no proof (the plant manager left them alone in the room).

We were supposedly prepared for an event where one of our boot-up drives crashed, however the backup unit and the main unit were the two which crashed. It took about a month and a half and 4 refurbished drives later to get us up and running.

A few weeks after we were up and running fully, there was an electrical fire in the manufacturing plant, at the point were the electricity came into the plant. Fortunately, the system was saved from being fried, but we had to deal with the soot from the fire.

Because there was no electricity, we were able to bring in diesel electric generators and get the computers up and running (since our computer was accessed by our salesmen and by company P's other manufacturing plants). The generated electricity was "dirty" and our UPS consistently complained and would go online.

Also, during the evenings when no one was around, the electricity consumption decreased, and somehow the generator would detect that and do something to the electricity such that the UPS would kick in. For a week we came into work with the UPS beeping in morse code SOS, and our system would be down, until we temporarily solved the problem by leaving all the lights and personal computers on during the evenings.

Needless to say, it was an exciting and unpredictable summer, with lots of long hours, frustrations, and rewards. And company P is still operating today.

Risks? No matter how prepared you are, you are never prepared enough.

Robert Telka, Computing & Communications Services, Carleton University, Ottawa, Ontario, Canada watpod13@ccs.carleton.ca ug930017@mach.scs.carleton.ca

Digital Detritus

Eric Sosman x4425 <eric@tardis.hq.ileaf.com> Thu, 10 Mar 94 16:12:48 EST

In <u>RISKS-15.64</u>, jcr@msen.com (John C. Rivard) reports that "A News editor had a composting room worker sneak along a copy of the digital photo file, without the knowledge of the Free Press."

I wondered idly what kind of pitchfork would be best for digital compost, but came to no earth-shaking conclusions. Despite mental ferment, I made, as they say, no hay. Eventually, I moved on to the next article ... in which dnorman@apple.com (Don Norman) speculated that "Maybe appalling grammar is bad language design."

There are moments when the enjoyment to be derived from digitized debate seems to outweigh almost any RISK.

Eric Sosman, Interleaf, Inc., Prospect Place, 9 Hillside Ave. Waltham, MA 02154 eric@ileaf.com

Digital Destritus (Re: RISKS-15.64)

Stephen D Crocker <crocker@tis.com> Thu, 10 Mar 94 13:21:31 -0500

> ... a composting room worker ...

Hmmm... We always known what news people handle, but it's nice to know they know too.

I don't recall the outcome, but there were some lawsuits a while ago concerning the government's right to paw through your trash after you put it on the street. Is compost material protected by intellectual property laws or

the first amendment? I suppose one could argue about a right to privacy...

Steve

[An interesting question relates to information residues and remanence. When can useful information be reconstructed from compost? PGN]

✓ Maybe appalling grammar is bad language design (RISKS-15.64)

<MJackson.wbst147@xerox.com> Thu, 10 Mar 1994 11:29:04 PST

- > With words that are homonyms, so the same spelling indicates contraction
- > and possession, the rule is that contraction wins use of the '. Hence,
- > "It's not its fault," where "it's" is a contraction and "its" is a
- > possessive.
- > Try explaining that to a non-native speaker of English. Hell, try
- > explaining that to a native speaker.

In either case, try explaining it *correctly*. There is no such "contraction wins" rule. "Its", like "his" and "her," is a possessive pronoun, not a noun requiring "'s" (or "'", if already ending in s) to form a possessive. One does not even think of writing "I threw hi's ball over the fence," notwithstanding the fact that "his" has no homonym.

- > If English weren't so stingy with symbols and used different symbols for > possession and contraction, then we wouldn't have any problem.
- An extremely unlikely statement on its face, and completely unsupported by the preceding argument.

Mark Jackson

✓ Which Johnson? (was Maybe appalling grammar is bad language design)

Alayne McGregor <mcgregoa@cognos.com> Fri, 11 Mar 1994 09:31:49 -0500

I would have more sympathy with Don Norman's comments about bad language design (RISKS-15.64) if he hadn't confused the great lexicographer with a [...] runner.

Samuel Johnson, please!

Mr. Norman has, however, produced an interesting analogy. Any software designer who thinks that his/her design will survive many iterations of fixes and upgrades might look at the evolution of languages for a cautionary counter-example.

Alayne McGregor, mcgregoa@cognos.com

RISK to freedom of information

Philip Overy <PJO@ib.rl.ac.uk> Fri, 11 Mar 94 09:53:33 GMT

"Freedom of information" means literally "freedom to defend yourself", ie "the right to live". States can falsify information on a grand scale (eg make computers) and do pretend to respect human rights (which I would argue is a weak claim, but the UK and the USA do indeed make that claim, and spend a fairly derisory but not non-existent sum to "prove" it); if you can attribute heinous crimes, such as child pornography, to someone, then you can destroy them. Clipper in effect destroys the value of computer evidence ("it must be faked"), so I am glad in a way that the public scepticism of computer "evidence" is about to be reinforced. I don't believe that the law enforcers will thank Clinton, once they realise the true effect of Clipper on their cases - everyone will claim that the police "of course" knew all about their personal life and then falsified suitable evidence to substantiate a tailor-made case. They will edit their own version and insert points at which the police "made it all up" (as they do in many non-computerised defences). I await with interest the first defence on these lines when Clipper hits the streets.

Phil Overy, Rutherford-Appleton Laboratory

Re: Clipper (Henson, RISKS-15.64)

Mark Eckenwiler <eck@panix.com> 11 Mar 1994 03:02:02 -0500

Since Mr. Henson speaks of "Clipper" (and not Skipjack generally), I assume he's referring strictly to telephonic communications. He's incorrect in implying that a Magistrate Judge can issue a wiretap warrant; Title III makes quite clear that they *cannot*. See _In re United States , 10 F.3d 931 (2d Cir. 1993).

>These magistrates (who are *not* judges, but work for the US Attorney's >office) tend to be busy, or lazy or corrupt or all three.

Mr. Henson also misstates the facts here. Magistrate Judges most assuredly do not work for the US Attorneys nor for the Department of Justice. They are Article I judicial officers; in my experience, they are no more or less "lazy or corrupt" than life-tenure, Article III federal judges.

And for the record, I oppose Clipper.

Magistrate-Judges (hkhenson, RISKS 15.64)

"Daniel B. Dobkin" <dbd@ans.net>

Fri, 11 Mar 94 11:38:41 EST

In RISKS-15.64, hkhenson notes that

The risk under Clipper is that your private communications will be protected by the *weakest* link in the chain--one of the thousands of low level Magistrate-Judges among whom corrupt or zealous law enforcement agents shop for warrants and will shop for keys.

This is hardly the only risk under Clipper, nor are the federal magistrates necessarily the weakest link in the chain: your conclusion is based on an incorrect understanding of the law and the role of U.S. Magistrate-Judges.

These magistrates (who are *not* judges, but work for the US Attorney's office) tend to be busy, or lazy or corrupt or all three.

The magistrates *are* judges. They do not work for the U.S. Attorney's office, but for the United States District Court. The magistrates are appointed by the District Court which they serve, for nine-year terms; the District Court judges (who appoint the magistrates) are appointees of the President, and serve for life. Magistrates are as well-qualified as the judges they serve, and have the same duties, responsibilities, and powers. They do tend to be busy; in my experience, they are not likely to be any more lazy or corrupt than any other federal judge.

As in this case, even if the law is *directly quoted* in search warrant affidavits or key requests, and these laws *expressly forbid* granting warrants or key requests under the conditions cited, the magistrate may not even read the supporting affidavit before approving it. He is *very* unlikely to read or consider the underlying laws when granting a request.

This is no more true of a federal magistrate than of any other judge, in either the federal or state court systems. As a rule, judges *do* try to make sure that the application is lawful and that the rules for granting it are applied appropriately. Sometimes a bad application gets through, and some judges unquestionably treat such applications more favorably than others. This is a general problem with "the system" and is not unique to Clipper. There *might* be an enhanced risk with Clipper because the bench (almost by definition) is inhabited by generalists who are called upon to be "instant experts" in many areas; they must rely on others to provide them with sufficient technical insight to allow an informed decision. Sometimes that insight is provided entirely by the applicant; very often, it is provided by the judge's law clerk.

The key escrow agents provide no protection whatsoever since they simply fill orders from agents with approved applications.

This, in fact, is a much more troubling weakness with the Clipper proposal, and one which has been discussed at length in other fora. While Clipper does introduce some very weak links into the security chain, judicial oversight is not one of them --- that particular link is not changed at all. (One could even argue that because the technology makes wiretaps so much easier, judges might actually be less inclined to approve every application that comes their

way.)

\dbd

13th Intrusion-Detection Workshop

Teresa Lunt <lunt@csl.sri.com> Thu, 10 Mar 94 10:35:03 -0800

THIRTEENTH INTRUSION-DETECTION WORKSHOP
May 19-20, 1994
SRI International
Menlo Park, California, USA

You are invited to attend a two-day workshop on intrusion detection to be held at SRI International in Menlo Park, California on May 19-20, 1994, which are the Thursday and Friday following the 1994 IEEE Symposium on Research in Security and Privacy in Oakland, California. This will be the thirteenth in a series of intrusion-detection workshops. The workshop will begin at 9am and will conclude at 5pm on Thursday, and will be from 9am to 2pm on Friday.

The workshop will consist of several short presentations as well as discussion periods. If you and/or your colleagues wish to attend or have questions, please send E-mail to Liz Luntzel, luntzel@csl.sri.com, or call her at 415-859-3285. Specify your name, title, affiliation, address, and phone number. You can also send us a fax at 415-859-2844. Directions to SRI will be provided on request.

If you have any progress to report on an intrusion-detection project or some related work that would be appropriate for a short presentation, please indicate the title and a paragraph describing your proposed talk. You can also indicate suggestions for discussion topics.

There will be a \$100 charge for the workshop. This fee includes lunches in SRI's International Dining Room. Please send your check to Liz Luntzel, EL248, SRI International, Computer Science Laboratory, 333 Ravenswood Avenue, Menlo Park, California 94025-3493.

First announcement of COMPASS '94, program and info

Teresa Lunt <lunt@csl.sri.com> Fri, 11 Mar 94 15:17:31 -0800

COMPASS '94

June 27 - July 1, 1994

Ninth Annual Conference on Computer Assurance
Systems Integrity, Software Safety, and Process Security
National Institute of Standards and Technology, Gaithersburg, MD

COMPASS Sponsors IEEE Aerospace and Electronics Systems Society IEEE National Capital Area Council

In Cooperation With British Computer Society

PROGRAM RELATED INFORMATION FOLLOWS.

FOR General Information, Registration Form, and Hotel Info, PLEASE SEND E-mail to mclean@itd.nrl.navy.mil or FTP from RISKS archives on CRVAX.SRI.COM

CD RISKS:

GET compass.94

Conference Sponsors

Arca Systems, Inc. ARINC Research Corporation Control Systems Analysis, Inc CTA, Inc. Logicon, Inc. National Institute of Standards and Technology Naval Research Laboratory Naval Surface Warfare Center Systems Safety Soc. TRW Systems Division U.S. General Accounting Office

COMPASS is an annual conference committed to bringing together researchers, developers, and evaluators who work on problems related to specifying, building, and certifying high-assurance computer systems. What distinguishes COMPASS from similar conferences is its emphasis on bridging the gap between research and practice. Researchers are provided an opportunity to present results, new theories, and new technologies to both other researchers and practitioners who can put them to practice. They can also learn from practitioners of new research problem domains and of problems encountered in building real systems. Practitioners have an opportunity to share lessons learned, to learn of new research, and to influence future research.

Welcome to COMPASS 94, the ninth in a series of annual symposia on Computer Assurance. This year's conference focuses on both the use and assessment of formal methods and on alternatives to formal verification in a variety of critical areas:

- * Safety
- * Reliability
- * Fault Tolerance
- * Concurrency and Real Time
- * Security

At COMPASS, the diverse program and small conference atmosphere provide plenty of opportunity for audience and speakers to mingle and share their experiences. The audience bring their own wealth of knowledge, and interchanges among industry, members of government agencies, and academia provide unique opportunities to discuss current requirements and future needs. We invite you to participate and increase the benefits of COMPASS by your attendance.

*** MONDAY, 27 JUNE

8:00 am Registration Opens

9:00 am - 4:00 pm Tutorial (Lunch on your own)

1. "Formal Software Development Using Z", John McDermid, University of York

Much has been written about the benefit of formal methods for developing high

integrity software -- but there are relatively few examples of successful use of formal methods on large scale projects. This tutorial demonstrates that cost-effective formal software development is now possible, using Z and a refinement approach into Ada that is supported by two tools: CADiZ and ZETA. CADiZ supports the production and analysis of Z specifications. ZETA supports formal, rigorous or informal stepwise development of Ada from Z specifications (in compliance with the UK Interim Defence Standard 00-55) in a cost-effective way that enables the user to determine the level of rigor for the refinement. Examples will be offered, and the tools will be demonstrated in support of the presentation.

*** TUESDAY, 28 JUNE

8:00 am Registration Opens

9:00 am - 4:00 pm Tutorials (Parallel Sessions) (Lunch on your own)

2. [FULL DAY] "Software System Evaluation and Certification"
Hans-Ludwig Hausen, GMD (German National Research Center for Computer Science)

Software quality evaluation and certification have been recognized as important issues for the American, European and especially the Japanese software industry. This tutorial focuses on the methods and tools for the evaluation and assessment of software products and processes. Particular emphasis is given to identifying and selecting software characteristics and metrics and the handling of evaluation methods and tools. The impact of the SEI Capability Maturity Model, SPICE, ISO 9000 series, ISO 12119, ISO 9126 and the EVALUATION METHOD will be discussed in detail.

9:00 am - 12 Noon [HALF DAY]

3. "Software Hazard Analysis", Nancy Leveson, University of Washington

The goals and techniques of software hazard analysis will be presented and general procedures, including new state machine algorithms, discussed. Topics include Software System Hazard Analysis and Software Requirements Analysis. Finally, an example using a real application (TCAS II) will be offered.

12 Noon - 1:00 pm Lunch (on your own)

1:00 pm - 4:00 pm [HALF DAY]

4. "Practicing Software Safety in a Virtual Corporation" Frank Houston, Weinberg, Spelton, & Sax, Inc.

In this half-day tutorial, the participants will play the roles of entrepreneurs who are developing a new medical device. The goal is for participants to develop the preliminary concept for the device, including safety requirements. If time permits, participants will develop a plan for validation and verification of the device, addressing regulatory Good Manufacturing Practice issues in the process.

*** WEDNESDAY, JUNE 29

8:00 am Registration and Tools Fair Open (tools that will be exhibited are

listed at the end of this Agenda)

9:30 am - 10:00 am Welcoming Remarks

James H. Burrows, Director, Computer Systems Laboratory, NIST Jarrellann Filsinger, General Chair and John McLean, Program Chair

10:00 am - 11:00 am Keynote Address, Jerry O. Tuttle, VADM USN (RET.)

11:30 am - 1:00 pm SAFETY I

"Experience Applying the CoRE Method to the Lockheed C-130J Software Requirements", Stuart Faulk, Lisa Finneran, James Kirby (SPC) and James Sutton (Time Plus)

"AeSOP: An Interactive Failure Mode Analysis Tool", Stephen S. Cha (The Aerospace Corp.)

"A Development of Hazard Analysis to Aid Software Design", John McDermid and D. J. Pumfrey (University of York)

2:00 pm - 3:30 pm USE AND ASSESSMENT OF FORMAL METHODS

"Formal Methods in Language Design", David Guaspari (ORA)

"Case Study: Applying Formal Methods to the Traffic Alert and Collision Avoidance System (TCAS)", Joan J. Britt (MITRE)

"Formal Methods and Dependability Assessment", V. Stavridou, S. Liu, and B. Dutertre (University of London)

4:00 pm - 5:00 pm ALTERNATIVES TO FORMAL VERIFICATION

"Using Formal Methods to Derive Test Frames in Category-Partition Testing", Paul Ammann and Jeff Offutt (George Mason University)

"Application of an Informal Program Verification Method to Ada", Bruce Wieand (IBM) and William E. Howden (University of California)

5:00 pm Tools Fair Closes

*** THURSDAY, JUNE 30

8:00 am Registration and Tools Fair Open

9:30 am - 11:00 am FAULT TOLERANCE

"Centurion Software Fault Tolerance Design and Analysis Tool", G. Steve Wakefield (SRS), Roger Dziegiel (Air Force Rome Lab), and Laura L. Pullum (Quality Research Associates)

"Estimation of Coverage Probabilities for Dependability Validation of Fault-Tolerant Computing Systems", Cristian Constantinescu (Duke University)

"Formal Verification of an Interactive Consistency Algorithm for the Draper FTP Architecture Under a Hybrid Fault Model", Patrick Lincoln and John Rushby (SRI International)

11:30 am - 1:00 am CONCURRENCY AND REAL-TIME SYSTEMS

"State Minimization for Concurrent System Analysis Based on State Space Exploration", Inhye Kang and Insup Lee (University of Pennsylvania)

"Compositional Model Checking of Ada Tasking Programs", Jeffrey Fischer (Verdix) and Richard Gerber (University of Maryland)

"An Ounce of Prevention is Worth a Pound of Cure: Towards Physically-Correct Specifications of Embedded Real-Time Systems", Azer Bestavros (Boston University)

2:00 pm - 3:30 pm PANEL: SOFTWARE TESTABILITY FOR CRITICAL SYSTEMS

Dick Hamlet (Portland State University)
William E. Howden (University of California)
Keith Miller (Sangamon State University)
Jeffrey Voas (Reliable Software Technologies Corp.)

4:00 pm - 5:00 pm HARDWARE VERIFICATION

"A Formal Model of Several Fundamental VHDL Concepts", David M. Goldschlag (NRL)

"Experiences Formally Verifying a Network Component", Paul Curzon (University of Cambridge)

5:00 pm Tools Fair Closes

6:30 pm BANQUET, Speaker: Brian Randell (University of Newcastle)

*** FRIDAY, JULY 1

8:00 am Registration and Tools Fair Open 9:30 am -11:00 am SAFETY II

"Evaluating Software for Safety Systems in Nuclear Power Plants", J. Dennis Lawrence, Warren L. Persons, and G. Gary Preckshot (Lawrence Livermore National Laboratory)

"An Approach for the Quality Analysis of Safety Specifications", Amer Saeed, Rogerio de Lemos, and Tom Anderson (University of Newcastle)

"Causality as a Means for the Expression of Requirements for Safety Critical Systems", Andrew Coombes, John McDermid, and Philip Morris (University of York)

11:30 am Tools Fair Closes

11:30 am - 1:00 pm SECURITY

"Covert Channels -- Here to Stay?", Ira S. Moskowitz and Myong H. Kang (NRL)

"An Experience Modeling Critical Requirements", Charles N. Payne, Andrew P. Moore, and David M. Mihelcic (NRL)

"On Measurement of Operational Security", Sarah Brocklehurst and Bev Littlewood (City University) and Tomas Olovsson and Erland Jonsson (Chalmers University of Technology)

1:00 pm Adjourn Technical Program

TOOLS EXHIBITED AT TOOLS FAIR

RiskWatch
AeSOP, ARiES
EVES
AdaWise, Penelope Romulus, Larch-Ada
McCabe Toolset
ModeChart Toolset
Centurion
RDD-100

Boundary Flow Covert Channel Analysis

INTERLOCKS

Conference General Co-Chairs:

Jarrellann Filsinger, Booz-Allen & Hamilton, H.O. Lubbes, NRL

Program Chair: John McLean, NRL Arrangements: Laura M. Ippolito, NIST

Publications: Ann Boyer, Control Systems Analysis

Publicity: Paul Anderson, Space and Naval Warfare Systems Command

Registration: Karen Ferraiolo, Arca Systems, Inc. Treasurer: Bonnie P. Danner, TRW Systems Division

Tutorials: John J. Marciniak, CTA, Inc. Tools Fair: Charles N. Payne, NRL

Program Committee Paul Ammann, George Mason University

George Dinolt, Loral

Jarrellann Filsinger, Booz-Allen & Hamilton

Virgil Gligor, University of Maryland

Li Gong, SRI International

Connie Heitmeyer, NRL

Jeremy Jacob, University of York

Carl Landwehr, NRL

Teresa Lunt, SRI International

John J. Marciniak, CTA, Inc.

John McDermid, University of York

John McHugh, Portland State University

Jon Millen, MITRE

David Parnas, McMaster University

John Rushby, SRI International

Ravi Sandhu, George Mason University

Jeannette Wing, Carnegie Mellon University

Board of Directors Chair: Dolores R. Wallace, NIST

Vice-Chair: Anthony Shumskas, Logicon, Inc. Treasurer: Dario DeAngelis, Logicon, Inc.

Secretary: Judy Bramlage, U.S. General Accounting Office

IEEE AESS: Robert Ayers, ARINC, Inc.

IEEE NCAC: Arthur Cotts

Members: Michael L. Brown, Naval Surface Warfare Center;

Jarrellann Filsinger, Booz-Allen & Hamilton; Frank Houston, Weinberg, Spelton, & Sax, Inc.; H.O. Lubbes, Naval Research Laboratory



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 66

Thursday 17 March 1994

Contents

Hit the Wrong Key, become a Verb...

Peter Wayner

Aldrich Ames, Master Hacker?

Peter Wayner

"Clipper Compromised?" brief in Network World 14 Mar 1992

Christopher Wysopal

Sly Imposter Robs S.F. Man of Good Name

Mike Crawford

Fire knocks out phone service in LA

George Feil

Ease of Administering Phone Systems Leads to Risk of Sabotage

George Pajari

Nessy - same new trick

Bob Frankston

Super-ID and Surveillance

Mich Kabay

Caught with their pants down [de-picted by rabbit admirers]

Mich Kabay

Neo-nazi T.A.D. eavesdropping

Mich Kabay

Derivatives

Phil Agre

Followup report on TCAS incident in Portland

Lauren Wiener

Caller ID utility

Robert Morrell Jr.

New Security Paradigms Workshop: CFP and Correction

Catherine A. Meadows

Info on RISKS (comp.risks)

Hit the Wrong Key, become a Verb...

Peter Wayner <pcw@access.digex.net> Wed, 16 Mar 1994 15:40:25 -0500

The Wall Street Journal (3/16/94, pg 1) reported that Jan Pablo Davila lost at least \$207 million of Codelco, a state-owned Chilean company by typing the wrong financial transaction into his computer. He typed "buy" when he says he ment to type "sell". Now, all of Chile is obsessed with the mistake that cost 0.5% of Chile's GNP and the new word "davilar" is a verb that is "...loosely translated as 'to botch things up miserably.'"

Aldrich Ames, Master Hacker?

Peter Wayner <pcw@access.digex.net> Wed, 16 Mar 1994 15:33:56 -0500

The Washington Times (3/16/94,pg A3) reported:

CIA sources told the Washington Times that Mr. Ames used his CIA computer to make unauthorized entries into computers within the espionage branch and downloaded information about the CIA's operations in Europe, including the identity of undercover agents posing as businessmen.

The story goes on to say that they'll be tightening up access to this information in response to this problem. But later in the story, they note that they'll be loosening requirements for peering into the financial records of the agents. "New legislation would be required to permit secret searches into personal-finance and credit data without employee consent."

My prediction is that they will reverse both of these changes in a few years when they discover that 1) some operation abroad was hampered by lack of direct access to info at a critical time and 2) some employee was bribed/spindled or mutilated using the data that they got by peering through credit records.

This just illustrates the problems of maintaining secrets and building networks of trust. The CIA has a hard job ahead of them. The folks who are building a Clipper network and crossing their fingers that the centralized repository won't be compromised have an even tougher one.

✓ "Clipper Compromised?" brief in Network World 14 Mar 1992

Christopher Wysopal <Christopher_Wysopal@smtprouter.lotus.com>
15 Mar 94 16:22:48 ES

Clipper Compromised?

"Security Insider Report," a monthly newsletter published in Seminole, Fla., has reported that government officials are seeking to determine whether former CIA employee and alleged traitor Aldrich Ames may have sold information to the Russians about the government's secret key-escrow technology used in Clipper Chip chipsets and Capstone Tessera cards. The secret key-escrow technology, dubbed Skipjack, can be used to encrypt network voice and data.

Network World, March 14, 1994, Page 2

The RISK of secret algorithms and government key escrow being compromised may already be 100 percent.

- Christopher Wysopal

[Also noted by seaman@noao.edu (Rob Seaman). PGN]

Sly Imposter Robs S.F. Man of Good Name

Mike Crawford <crawford@scipp.ucsc.edu> Mon, 14 Mar 1994 11:35:07 -0800

"Sly Imposter Robs S.F. Man of Good Name", by Catherine Bowman, *San Francisco Chronicle*, 14 Mar 1994, p.1.

San Francisco attorney Charles Sentman Crompton II, dogged by a string of arrest reports, mysterious credit card bills and a fake ID, is fed up and frustrated - so frustrated, in fact, that he is taking Charles Sentman Crompton III to court. [...]

Using Crompton's name, address, and Social Security number, the man has opened charge accounts at local stores, rented an apartment and obtained a driver's license, Crompton says. He has allegedly run up nearly \$3,000 in purchases at Macy's, Radio Shack and other stores, buying a portable computer and other items. [...]

(The suspect has been repeatedly arrested and set free by local police for stealing cars, etc., and gave Crompton's name.) [...] (The real Crompton obtains the phony Crompton's driver's license after the suspect drops it while fleeing from a suspicious store clerk.) [...]

Crompton obtained a photocopy of that license, which he forwarded to the state Department of Motor Vehicles with a letter explaining the problem. He then asked for a new license with a different number.

The DMV obliged. Then in a monumental goof, the agency mailed the license to the other Crompton. [...]

(The article includes a photo of the real Crompton and a physical description of both men. Real Crompton states that phony Crompton could not possibly be a true Elvis fan like him.)

The punch line:

Crompton says he does not blame the system for allowing the case to snowball. Still, he worries about his credit record and being fingered for crimes he did not commit.

Hmm... I'd say that this is a built-in feature of the system.

Mike's doomsday speech:

"We are just entering the Information Age. Those who possess the information, those who dispense it, and those who know how to manipulate the information will be the rulers. Those who do not will be the peasants."

I conjecture that the DMV goof was caused by different people handling the task of reissuing the license without communicating the nature of the problem to each other. One clerk dutifully issued a request for a new license, and perhaps typed a memo explaining the problem. Another clerk printed the license and sent it to the address on file (along with the letter explaining the problem, so the phony Crompton was officially tipped off in writing by the state.)

The California DMV is one of the largest bureaucracies in the United States, and possesses one of the largest management information systems as well. Well-defined lines of communication to handle such exceptional situations probably do not exist. I'd say we're lucky it works at all for the normal case.

One solution might be a government debugging agency. There should be a single office that Crompton could go to, that would work with all of the government agencies and credit bureaus to straighten out the record.

Of course this agency would itself be a fertile ground for fraud.

Mike Crawford, Author of the Word Services Apple Event Suite crawford@scipp.ucsc.edu Free Mac Source Code: ftp sumex-aim.stanford.edu get /info-mac/dev/src/writeswell-jr-102-c.hqx

Fire knocks out phone service in LA

"George Feil" <feil@sbcm.com> Tue, 15 Mar 94 09:19:45 -0500

A news bulletin just in: A fire in a Pacific Bell switching complex has knocked out local phone service to most of Los Angeles, CA.

Those of us who recall the Hinsdale, IL fire of several years ago are already aware of the significant potential single points of failure in the U.S. telephone systems. Again, fire turns out to be the Achilles' Heel in this case.

It is ironic that while many financial firms (including my own) have remote disaster sites, and have had occasion to use them (we tested ours for the first time when the World Trade Center was bombed last year), telephone companies continue to use the "fortress" approach, beefing up security of non-redundant phone switches, instead. It doesn't appear to be effective enough, and fire will likely be the key element of disaster.

Ease of Administering Phone Systems Leads to Risk of Sabotage

George Pajari <pajari@faximum.com> Tue, 15 Mar 94 22:26:27 PST

The newer digital small-office phone systems (such as the Northern Telecom Meridian or NorStar units) reduce the system complexity and cost by enabling the system to be configured from any telephone (rather than from a terminal or other specialised interface).

While all of the critical settings are password protected, changing the password on phone systems seems to be even less popular than managing computer passwords.

While waiting for some friends at a local (very) up-market Chinese restaurant I noticed that the convenience phone provided patrons in the waiting area was a NorStar. Having little else to do while waiting I decided to try the factory-default master administration password. It worked. The surprise was that when I turned over the phone I saw the "Installed by" sticker of the local telco's "independent" customer premise equipment interconnect company (i.e. not some small fly-by-night operator but the largest vendor of such equipment in the province).

The RISK? Reprogramming their phone switch (a) to change the password and (b) not to ring on any (audible) extension when incoming calls arrive on their reservation lines could easily cost such a restaurant a significant chunk of its income (especially on a Saturday when even finding someone able to fix the problem once it was discovered could result in hours of delay, not to mention the time to type in the entire configuration again once the memory was wiped to get around the changed password).

George Pajari, Faximum Software, 1497 Marine Drive, Suite 300, West Vancouver, BC / Canada V7T 1B8 pajari@Faximum.COM / Tel: +1 (604) 925-3600

✓ Nessy - same new trick

<Bob_Frankston@frankston.com> Sun, 13 Mar 1994 18:02 -0400

Just as a reminder that doctoring photos is nothing new, there is a news story out of the UK on CNN saying that someone confessed (on his deathbed) that the famous Loch Ness Monster picture was a hoax. On one hand, it reminds us that as much as we like to think that all we do is new, it isn't. But it also puts the risk in perspective and makes us think about how these risks have been handled in the past. Alas, they are not handled all that well.

Super-ID and Surveillance

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 17 Mar 94 21:37:38 EST

Article by David Lyon in Canada's Globe and Mail, 94.03.17, p. A21:

"Super-ID: keeping and eye on everybody."

The author reports on Ontario government officials are considering providing citizens with a single universal identifier to replace the hodge-podge of driver's license, medical card and so on.

Key points:

- o Driving concern is fraud, especially by foreigners using Canadian medical insurance cards for free medical care.
- o Trend towards a "surveillance society" in which it is expected that governments and private industry have a right to as much information as they can gather about individuals, their preferences, behaviour and movements.
- o Risks of developing and using profiles of suspect behaviour and applying sanctions or suspicion to innocent people simply because they happen to fit a statistical pattern.
- o Single ID allows cross-relations among disparate databanks; could easily lead to abuse by commercial or other exploiters.
- o Countries differ in extent to which they require "papers":to be carried by citizens. France have used them for decades, Germans since 1987. Britain still resisting the universal ID, including DNA fingerprints. Australian proposal rejected in 1987.
- o Recent surveys in Canada indicate popular concern over privacy is rising; in 1993, a "survey by Ekos Associates showed that 52 per cent of Canadians are `extremely concerned' about privacy. Sixty per cent claim they have less privacy than 10 years ago, and 81 per cent of them attribute this to computer use."

The author ends his thoughtful, concise essay with a note on who shall determine whether a single ID is to be used. He urges everyone to "question the morality of the super-ID and its place in the trend toward a surveillance society. And we need to find out just how and why people feel threatened, diminished or fearful about things that on other levels--security, efficiency, convenience--seem so alluring.

The paper published this note about the author: "David Lyon is associate professor of sociology at Queen's University, Kingston [Ontario]. His latest book is _The Electronic Eye: The Rise of Surveillance Society_ (University of Minnesota Press, 1994).

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Caught with their pants down [de-picted by rabbit admirers]

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>

17 Mar 94 21:37:45 EST

An article from the Reuters News Agency appeared in Canada's _Globe and Mail_ newspaper for 94.03.17, p. A15:

"Who undressed Jessica Rabbit?"

It seems that officials at Walt Disney Co. are embarrassed because some of their animators got a little playful with Jessica Rabbit, the sultry lead in the semi-animated film, "Who Framed Roger Rabbit?" In one scene, the animators (or someone) removed Jessica's underwear in three frames during a pirouette which causes her skirt to ride up around her waist.

News of this ghastly descent into depravity seems to have caused hundreds of people to rush out and buy the \$40 CD of the film, depleting stocks at many retail outlets. As one viewer said after the L.A. Fox TV affiliate KTTV showed the three frames publicly on the 16th of March, "If that turned you on, it's time to see a psychiatrist."

[Seems to me that the RISK here is quality control failure more than anything specifically electronic. However, given the growing dependence of animators on computers to help overcome the drudgery of their craft, I can see all kinds of possibilities for bored technicians or crafty hackers. How about a new version of Snow White--showing what she was _really_ up to with those cute dwarves. What about _The Lady and the Tramp--After Hours_? Or _The Unexpurgated Little Red Riding Hood_?]

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

✓ Neo-nazi T.A.D. eavesdropping

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>
17 Mar 94 21:37:54 EST

>From the Canadian national newspaper, _The Globe and Mail_, 94.03.17, p. A2B.

"Ex-member of Heritage Front tells hearing of dirty tricks."

by R. Platiel (Globe and Mail reporter).

A disenchanted young former Nazi reported that the neo-Nazi Heritage Front group broke into telephone answering devices (T.A.D.s) used by anti-racism activists and recorded the phone numbers of correspondents. They then passed these numbers around among neo-Nazi supporters and harassed the victims. She claimed that some anti-racists were followed; others found that their employers had received phone calls alleging that they were "Bolsheviks."

[Most T.A.D.s have a 2-digit code at best. Not very challenging to crack.]

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Derivatives

Phil Agre <pagre@weber.ucsd.edu> Tue, 15 Mar 1994 11:03:05 -0800

The new issue of Fortune contains a long article about the potential risks of derivatives, which are complex types of financial deals that depend on the values of certain underlying assets, such as currencies, commodities, or composite entities like stock indexes. The full reference is:

Carol J. Loomis, The risk that won't go away, Fortune 129(5), 7 March 1994, pages 40-57.

At the moment, there exist outstanding derivatives contracts on assets whose total value is about \$16 trillion dollars, about 2.5 times the United States' GDP. The problem is that nobody really understands how derivatives work. They only exist in the first place because of big computers and global data networks (see Risks 14.87). In theory, they allow firms to manage the risks of global business by hedging against potentially damaging fluctuations in commodity prices, interest rates, currency exchange rates, and so forth, and this can be a good thing. In practice, it is difficult to do this right. Moreover, the nature of derivative contracts entails increasing levels of interconnection in the world financial system, with the solvency of each major player frequently contingent on the ability of numerous other players to make good on complex contracts. A serious misjudgement at a large bank, on the order of the savage losses recently incurred through bungled oil-price hedging at the German firm Metallgesellschaft, could conceivably propagate through the entire system.

It actually gets worse from there, as Loomis explains at some length. Regulation is nearly nonexistent, largely because nobody knows how one *could* regulate such things. Reporting requirements are derisory as well. In short, the global economy is wound up real tight. To be sure, market forces are bringing an urgent profusion of risk management strategies. The big question is whether the prudence of individual players is adequate to prevent the total system from collapsing in case of some exogenous event, or simply because there's an angle nobody figures out until it's too late.

Phil Agre, UCSD

PS. The same issue of Fortune contains some advice for companies wishing to engage in commercial activity on the Internet.

Followup report on TCAS incident in Portland

Lauren Wiener <lauren@reed.edu> Wed, 16 Mar 94 19:00:26 -0800

>From the Oregonian, March 14, 1994, p. B3: [I'm in square brackets counting risks. LRW]

"FAA wants to know why system sent 2 jets toward each other

A collision course alarm sounded in the Portland incident, but the equipment's subsequent response has officials baffled A system designed to avert air collisions sent two planes heading toward one another near Portland Int'l Airport, and federal authorities are trying to figure out why. The Feb. 3 incident involved an Alaska Airlines jetliner and a HorizonAir commuter jet. Each plane was equipped with the Traffic Collision Avoidance System, which alerts pilots to other air traffic and sounds an alarm if there is a chance of a collision.

"The question is not whether TCAS did its job. The question is why did the logic of TCAS tell the upper plane to go down and the lower plane to climb," said Dick Meyers, a Federal Aviation Administration spokesman based in Renton, Wash. A crash would not have resulted if the pilots had continued obeying the instructions of the system, but the planes would have come uncomfortably close, FAA officials said.

Alaska Airlines pilot Thomas Hedrick had been instructed by an air traffic controller to climb to 9,000 feet and level off. At the same time, a HorizonAir commuter jet piloted by Brian Penwell was approaching the airport and was instructed to descend to 10,000 feet and level off.

In both planes, the FAA-required collision avoidance alarm sounded -- a common occurrence in the traffic-congested skies around airports -- letting the pilots know they were too close to other aircraft.

[Risk 1 -- many false alarms. LRW]

Then a second alarm sounded indicating the aircraft were on a potential collision course. Rather than advising the pilots to level off, the system instructed the higher-flying plane to descend below the lower-flying plane and the lower-flying plane to climb above the other.

[Risk 2 -- uncoordinated solutions. LRW]

An air traffic controller noticed the HorizonAir plane descending toward the Alaska plane and ordered the pilot to level off.

"I told him we could not because we were receiving a Resolution Advisory," Penwell wrote in a report filed with the FAA. A Resolution Advisory in this case was the system's directive to descend.

[Risk 3 -- unclear who or what is in charge. LRW]

Penwell said he finally saw the Alaska plane and banked to the left at about 9200 feet. Penwell estimated that the planes came within about a mile of each other."

Caller ID utility

"Robert Morrell Jr." <bmorrell@isnet.is.wfu.edu> Fri, 11 Mar 1994 19:35:05 -0500 (EST)

An anonymous contributor recently denigrated the utility of caller ID in stopping obscene callers, believing instead that the real purpose is to swell

the business telephone data banks. Yet in the note it is recognized that the uility for catching obscene callers is decreasing "as would be callers catch on".

Forgive me, but does that mean they are modifying their behavior? If it inconveniences them, discourages the casual obscene caller, has it not done its task?

The risks of this logic is clear... discard a technology that is doing what it was intended to do because someone else is making (horrors) money.

Bob

✓ New Security Paradigms Workshop: CFP and Correction

Catherine A. Meadows <meadows@itd.nrl.navy.mil> Thu, 17 Mar 94 14:06:10 EST

Note: The address of the second Program Chair, Eric Leighninger, has changed since this announcement appeared in SIGSAC Review and elsewhere. The address listed below is the correct one.

CALL FOR PAPERS

A workshop sponsored by ACM SIGSAC and DOD

NEW SECURITY PARADIGMS '94

Paradigm shifts disrupt the status quo, destroy outdated ideas, and open the way to new possibilities. This workshop explores new ways of looking at computer security, hoping to develop transcendent solutions that provide the interoperability and flexibility users need in trusted systems.

> AUGUST 3-5, 1994 Stone House Club Little Compton, R.I.

New Security Paradigms '94 provides a creative and constructive workshop environment at a small seaside inn for 20 researchers. Dress is casual. The workshop fee of about \$450 includes room, meals, and workshop materials.

To participate, submit a research paper or a 5-10 page position paper (5 copies) to one of the two program chairs by March 26, 1994. The Program Committee will referee the papers and notify authors of acceptance by June 11, 1994. Proceedings will be published by ACM.

Program Chair: John Dobson
Computing Science Dept.
University of Newcastle
Newcastle NE1 7RU U.K.
(+44) 91 222 8228

email: John.Dobson at newcastle.ac.uk
Program Chair: Eric Leighninger NOTE NEW ADDRESS!

334 Linwood Ave Apt.3

Newtonville, MA 02160 (617) 558-1412

Workshop Chair: Hilary H. Hosmer, Data Security, Inc.

Publications Chair: Catherine Meadows, NRL

Scholarships: Ravi Sandhu, George Mason University

Treasurer: Steven Cha, Aerospace

ACM SIGSAC Liaison: Dixie Baker, Aerospace



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 67

Friday 18 March 1994

Contents

Hazards on the Superhighway

Erskine Widemon

The RISKS of whale removal

Tom Mahoney via Mark Stalzer

The Handmaid's Tale, Giuliani-Style

Chris Kreussling

IRS Surveillance

J. Cooper

Risk Conference - Two for the price of one!

Patrick J. O'Toole

911 (again)

Richard Johnson

Re: Clipper Compromised

Dorothy Denning

It's Apple and it's grammar.

John Oram

L.A. phone fire (a.k.a. "Risks of believing ...)

Lauren Weinstein

RSAREF/RIPEM Free and Legal Worldwide

Jim Bidzos

CERT ADVISORY - MD5 Checksums

Info on RISKS (comp.risks)

Hazards on the Superhighway

Erskine Widemon <tzw2446@ddrw.dla.mil> Fri, 18 Mar 94 10:32:52 PDT

The following incidents were mentioned in the March 14, 1994 Modesto Bee.

- Laurie Powell joined an on-line service to discuss the joys and pitfalls of raising children. An elusive cyberstalker called Vito has threatened her life, sent her pornographic e-mail and may be following her around the

country.

- Larry Greenberg of New York could have lost his job when someone sent his boss a fax from a phony law firm accusing him of being a convicted rapist and child molester. Greenberg suspects the fax was sent by an on-line foe.
- A 14-year-old New Jersey girl was forced off the network last month after continuing to receive unwanted computer-generated sexual images of young boys.
- Evelyn McHugh, a New Jersey housewife, discovered a Chicago man was sending obscene messages in her name.
- A 14-year-old Boston boy disappeared after running away to meet a man in Texas who sent him on-line love letters and airline tickets.

Erskine Widemon

The RISKS of whale removal

<stalzer@macaw.hrl.hac.com>
Fri, 18 Mar 1994 08:33:48 +0800

This has absolutely nothing to do with computers, but it is heartening to know that our industry isn't the only one that does foolish things. -- Mark

---- Begin Included Message -----

The Farside comes to life in Oregon.

I am absolutely not making this incident up; in fact I have it all on videotape. The tape is from a local TV news show in Oregon, which sent a reporter out to cover the removal of a 45-foot, eight-ton dead whale that washed up on the beach. The responsibility for getting rid of the carcass was placed on the Oregon State Highway Division, apparently on the theory that highways and whales are very similar in the sense of being large objects.

So anyway, the highway engineers hit upon the plan--remember, I am not making this up--of blowing up the whale with dynamite. The thinking is that the whale would be blown into small pieces, which would be eaten by seagulls, and that would be that. A textbook whale removal.

So they moved the spectators back up the beach, put a half-ton of dynamite next to the whale and set it off. I am probably not guilty of understatement when I say that what follows, on the videotape, is the most wonderful event in the history of the universe. First you see the whale carcass disappear in a huge blast of smoke and flame. Then you hear the happy spectators shouting "Yayy!" and "Whee!" Then, suddenly, the crowd's tone changes. You hear a new sound like "splud." You hear a woman's voice shouting "Here come pieces of...MY GOD!" Something smears the camera lens.

Later, the reporter explains: "The humor of the entire situation suddenly gave way to a run for survival as huge chunks of whale blubber fell everywhere."

One piece caved in the roof of a car parked more than a quarter of a mile away. Remaining on the beach were several rotting whale sectors the size of condominium units. There was no sign of the seagulls who had no doubt permanently relocated to Brazil.

This is a very sobering videotape. Here at the institute we watch it often, especially at parties. But this is no time for gaiety. This is a time to get hold of the folks at the Oregon State Highway Division and ask them, when they get done cleaning up the beaches, to give us an estimate on the US Capitol.

Tom Mahoney, #9, Coast Guard Sqn.1/Div.13 CatLo

---- End Included Message -----

★ The Handmaid's Tale, Giuliani-Style

Chris Kreussling <70700.266@CompuServe.COM> 18 Mar 94 09:26:45 EST

The following appeared in the New York Times on Tuesday, March 1, front page of the Metro Section (page B1). I haven't seen reference to this in Risks digests since then. And if there's been anything about it since in the local press, I've missed it.

My comments and questions:

- Anyone know more about this than appeared in the Times?
- Those with the *technical* ability to affect Board of Ed funding had no *legal* authority to do so. The design of the system and its security does
- not reflect the legal and political boundaries of the organizations it's supposed to serve.
- Probably easy to overlook one budget code out of "399 different budget categories." Unless they were informed by the administration, the agency and personnel who actually installed the change probably didn't know its full impact. They were "just following orders" ...
- The funds were not just "frozen" they were "transferred" to another account. I think the technical term is "stealing"? The Mayor, his administration, and the City Comptroller violated state law. Are there computer-specific laws they may also have broken? Wire fraud, for example?

Giuliani Tries Electronic School-Spending Freeze, by Josh Barnabel

Without warning the Board of Education, the Giuliani administration last week loaded software on a computer accounting system to block spending on school supplies. But the administration reversed the spending freeze after the Board considered legal action ...

School officials said they discovered that the \$68 million spending freeze had been imposed only when budget analysts ... noticed that spending authorizations were rejected by the city's accounting system for lack of funds ...

At the direction of the Mayor and the city's Comptroller, the [Financial Information Services Agency] loaded new software on the city's accounting system after business hours on Thursday. The software sent

instructions to the city's computers blocking spending of 90 percent of the available funds in 399 different budget categories for all city agencies, from supplies and materials, to out-of-town travel, to temporary service and consulting contracts.

The software in effect froze the school system's checking accounts, and transferred the available balances into reserve accounts controlled by the Mayor ...

The board receives less than half its money from city taxes, and is not required to submit its detailed line-item budget to the Mayor or the City for approval ...

IRS Surveillance

<j.cooper6@genie.geis.com> Fri, 18 Mar 94 08:12:00 BST

>From COMMERCE BUSINESS DAILY, 940317 (Government notice of bids)

< ------< Department of the Treasury (DY), Internal Revenue Service, Constellation Centre, 6009 Oxon Hill Rd., Rm. 700, M:P:O:S Oxon Hill, MD 20745

< 36 -- REMOTE DIAL NUMBER RECORDERS

SOL IRS-94-0051 POC Shirley Campbell, Contract Specialist, (202) 283-1144.

The Internal Revenue Service intends to procure 28 remote telephone data collection units, including software. Capable of collecting and storing information from the target line on at least 700 telephone calls (time of call, length of call, number dialed, caller ID, call progress tone detection, etc.). The unit must be no larger than 5.9x1.5x3.2 inches.

The unit is controlled and records are transmitted through the dial- up line through a computer modem. The instrument must be transparent to the target line. The unit will be powered through the dial-up line.

100% Small Business Set-Aside. Telephone requests for the solicitation package will not be accepted. (0075)

[Great for identifying anonymous callers who request information on whether illegal acts must be declared, and other such revealing queries? PGN]

Risk Conference - Two for the price of one!

Patrick J. O'Toole <potoole@consultant.win.net> Thu, 17 Mar 1994 16:11:47

I recently registered for the upcoming Software Engineering Institute (SEI) Conference on Software Risk and provided my Master Card information for billing purposes. About a week later, I received a confirmation letter and receipt from the SEI; two days later, I received a second confirmation letter and receipt.

Since the registration and payment numbers were different on the two receipts, I suspected a double booking/billing may have occurred, and called the SEI to rectify the problem. After looking into the situation, the SEI informed me that I had tripped a bug in a program which resulted in my being double registered, but *not* double billed. They assured me that I was the only one affected, and that the problem had indeed been resolved.

Today I received two separate invitations to participate in an upcoming Software Engineering Process Group meeting. I am not planning to attend this particular event, but if anyone is interested in a "buy one, get one free" offer, please give me a call!

✓ 911 (again)

Richard Johnson <rdj@plaza.ds.adp.com> Mon, 14 Mar 1994 07:37:53 -0800 (PST)

Yeah, we've beaten 911 problems to death historically, but it's a change from Clipper. :=)

I have a friend. His family and mine are quite close. We call each other's houses daily, sometimes multiple times in one day. His phone number begins 591-1xxx.

As you guessed, about once a month, something happens with the phone company switching, and we get 911--as a wrong number. So far the emergency response people have been quite nice about this, and I haven't seen any penalty-type charges on our phone bill.

The risks:

Aside from the obvious one, that we're discussing a safety-critical system, is the sheer volume of calls this represents. Ten thousand different phone numbers could get automatically diverted to 911. If we figure 500 hours each month when people are awake and calling (that's 16 a day), and each one gets redirected once a month, then 911 must be seeing a wrong number every three minutes!

No wonder they're so nice about it...

Richard Johnson (rdj@plaza.ds.adp.com) (richard@agora.rain.com)

Re: Clipper Compromised

Dorothy Denning <denning@chair.cosc.georgetown.edu> Fri, 18 Mar 94 09:52:54 EST

<u>RISKS-15.66</u> included a brief from "Network World," which referenced a story in the "Security Insider Report" suggesting that Aldrich Ames could have had

access to Clipper's classified SKIPJACK algorithm or Clipper keys. A New York Times reporter asked me about this rumor a few weeks ago, and the whole idea struck me as so obviously absurd that I could hardly stop laughing. Nevertheless, I did check it out with people who would know. They confirmed what I thought. The whole rumor is total nonsense.

What I don't understand is why people persist is spreading rumors and speculation that have no basis and don't even make sense.

Dorothy Denning

✓ It's Apple and it's grammar.

John Oram <oramy92@halcyon.com> Fri, 18 Mar 1994 00:24:57 -0800

This was in the TidBITS newsletter (#217/14-Mar-94). Evidently the AppleScript creators don't read this newsgroup...

- >**John Baxter** <jwbaxter@pt.olympus.net> writes:
- > I've run into something that grammar mavens may find interesting.
- > Consider this correct [English version] AppleScript code:
- > tell word 4 of paragraph 2 of document 1 of application
- > "Scriptable Text Editor"
- > get it's text
- > end tell

>

- > Here, Apple has managed to make AppleScript syntax so English-like
- > that it commits the all-too-common mistake of using "it's" instead
- > of "its" as the possessive.

>

> You can of course also write that statement as:

> get the text of it

800 000 0000 0000

>

- > That sounds terribly stilted, but at least avoids the incorrect
- > use of the contraction in place of the possessive. One of the
- > amusing things is that Apple has the potential of running into
- > such problems in each language for which they provide an
- > AppleScript dialect.

L.A. phone fire (a.k.a. "Risks of believing all news reports...")

Lauren Weinstein <lauren@vortex.com> Thu, 17 Mar 94 21:02 PST

- > From: "George Feil" <feil@sbcm.com>
- > A news bulletin just in: A fire in a Pacific Bell switching complex
- > has knocked out local phone service to most of Los Angeles, CA.

The fire's impact was considerably overstated by press accounts. It occurred in the downtown L.A. "Madison" C.O. complex (in particular, LSAN-0470T), which is one of several downtown high-rise switching centers. The fire knocked out primary and secondary power supplies that (unlike many of the other supplies in the building, apparently) were co-located.

Failure of SS7 links caused disruption of interoffice service for customers whose local subscriber lines were served by that office, and wider disruption of 911 service throughout a broader portion of the L.A. area, since the citywide 911 center is downtown. There was also apparently some limited long-distance access problems to some areas for some carriers.

Media and local telephone operators quickly began publicizing local direct dial emergency numbers to offset the 911 failure. There were no reports that I heard of any serious problems relating to the 911 disruption. Some operations were switched to secondary facilities in other areas.

Outside of the 911 problems, most areas of the city and the surrounding metro area (except the immediate downtown area served by Madison) noticed few obvious effects.

--Lauren--

✓ RSAREF/RIPEM Free and Legal Worldwide

Jim Bidzos <jim@RSA.COM> Fri, 18 Mar 94 03:32:48 PST

For more info, contact Kurt Stammberger, RSA Data Security, Inc. 415/595-8782. To download RSAREF and RIPEM, send any message to rsaref@rsa.com or ftp from msu.edu

RSA DATA SECURITY ANNOUNCES DIGITAL SIGNATURE SOFTWARE THAT IS FREE AND LEGAL WORLDWIDE

Information superhighway gets free tool to authenticate information; an answer to Vice-president Gore's concerns over Internet break-ins

Redwood City, Calif. (March 21, 1994) - RSA Data Security, Inc. announced today a first: digital signature software that is both free and legal worldwide.

RSA applied for and received a "commodities jurisdiction," or CJ for a software package called RIPEM/SIG, which was built with RSA Data Security's RSAREF toolkit, a freeware package. A CJ, which is a ruling that the software falls under the Commerce Department's jurisdiction as opposed to the State Department, allows RIPEM to be freely and legally exported. Further, RSA has relaxed the use restrictions in its free crypto toolkit. RSAREF, and any

application built with it, may now be used in commercial settings as long as it is not sold or used to provide a direct for-profit service.

Digital signatures are produced using the RSA cryptosystem, which is a public-key cryptosystem. Each user has two keys - one public and one private. The public key can be disclosed without compromising the private key. The RSA cryptosystem was invented and patented in the late 1970's by Drs. Rivest, Shamir, and Adleman at the Massachusetts Institute of Technology.

Electronic documents can be "signed" with an unforgeable "signature" by using a document/private-key combination to produce a signature unique to the author/document. Anyone, by using only RIPEM and the public key of the author, can verify the authenticity of the document.

Applications of digital signatures are endless. One reason that the paperless office has never materialized is that paper must still be printed so that handwritten signatures can be applied. RSAREF and RIPEM solve that problem. Expense reports, any electronic forms, administrative documents, even tax returns can be electronically signed to speed electronic document flow and eliminate fraud. Information on the Internet can be signed and verified to prevent spoofing. Recently, unauthenticated messages at Dartmouth College caused an important test to be cancelled; messages impersonating faculty were sent out.

"Data mailed, posted, or put on servers on the Internet is inherently untrustable today," said Jim Bidzos, president of RSA. "Tampering with electronic documents takes no special skills, and leaves no trace. With the availability of a free, legal, and exportable tool such as RIPEM, there's no need for such a situation to continue. It can be used by individuals, corporations, and government agencies at no cost."

In a February 4th announcement, Vice-president Gore stated that the recent Internet break-ins could have been prevented with digital signatures. "Here they are," said Bidzos. Recently, cryptography has caused clashes between government and industry, over privacy issues, law enforcement concerns, and export issues. "The US government has approved this software for export," said Bidzos. "Clearly, it's no threat to them. And it's free."

Digital signatures can also be used to detect any virus before a program is executed, since any change whatsoever is detected.

The RIPEM application was developed using the RSAREF toolkit by Mark Riordan of Michigan State University. A Macintosh version, developed by Ray Lau of MIT, the author of the popular "Stufit" program, is also available. Versions for DOS, Unix, and all popular platforms are supported. "PEM" stands for Privacy Enhanced Mail, a published Internet standard for secure electronic mail. Other innovative applications can also be built with RSAREF and distributed at no cost. The full encryption-capable RIPEM is available only in the US.

RSA digital signatures are a standard feature of Lotus Notes, the Apple System 7 Pro Operating System, Novell NetWare, Microsoft Windows at Work, Windows NT, IBM System Security Products, DelRina PerformPro, WordPerfect InForms, SHANA InFormed, BLOC F3 Forms, Fischer International Workflow, and numerous other

products. Over 3 million commercial products in the market today already use RSA signatures under license from RSA Data. Other RSA licensees include General Magic, Hewlett-Packard, Oracle, Unisys, Digital Equipment Corp, Motorola, and numerous others.

RSA Data Security, Inc. designs, develops, markets, and supports cryptographic solutions toolkits and products. The company was founded by the inventors of the RSA cryptosystem in 1982 and is headquartered in Redwood City, California.

CERT ADVISORY - MD5 Checksums

CERT Advisory <cert-advisory-request@cert.org> Fri, 18 Mar 94 16:46:58 EST

CA-94:05

CERT Advisory March 18, 1994 MD5 Checksums

This advisory gives the MD5 checksums for a number of SunOS files, along with a tool for checking them. The checksums can be used to assure the integrity of those files.

The CERT Coordination Center is distributing these checksums because of an increasing number of incidents in which intruders who gain root access are modifying system files to install Trojan horses.

Moreover, intruders are modifying files so that they have the same checksum as the original file. This is possible because the standard "sum" program that comes with most UNIX systems was designed to detect accidental modifications to files and is not strong enough to prevent deliberate attempts to yield a specific checksum. The MD5 algorithm by RSA Data Security, Inc. is specifically designed to provide checksums that cannot be deliberately spoofed. We strongly recommend that sites install the MD5 software and use it to validate system software. More information on obtaining MD5 is given below.

The list of checksums in Appendix B of this advisory is provided for your convenience. In addition, we are providing a program that can assist you in checking your MD5 output against the values in the database. This checksum list is not complete. We have begun with a number of the more common locations for Trojan horses that we have seen in connection with the continuing "sniffer" attacks reported in CA-94:01 "Ongoing Network Monitoring Attacks." We intend to work with all vendors to expand this list and make more MD5 checksums widely available for anonymous FTP.

We encourage sites to consider installing a more complete package for monitoring system integrity, such as Tripwire from the COAST project (anonymous FTP on ftp.cs.purdue in "/pub/spaf/COAST/Tripwire") or the TIGER system from TAMU (anonymous FTP on net.tamu.edu in "pub/security/TAMU").

We will maintain a file, CA-94:05.README, that will contain pointers to additional databases and other updates as they become available.

[The entire Advisory is in RISKS-15.67MD5. Contact the CERT for further information. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 68

Tuesday 22 March 1994

Contents

Gambling

Phil Agre

I really like this guy's attitude

Alan Wexelblat

Phone Machines Call Each Other, Part Deux

Russell S. Aminzade

IRS Surveillance (Part II)

Zaiac

Dutch legislators trying to pull a fast one?

Ralph Moonen

Funny Money article in THE SCIENCES

Mich Kabay

Human Genome Project & Privacy

Mich Kabay

SGML--archiving style + content

Mich Kabay

Risk of bringing plastic cards through UK customs

Ross Anderson

RISKs of safe ATMs

Sidney Markowitz

Re: Hard-drive headache!

David M. Miller

Re: The RISKS of whale removal, copyrights

Matthew B. Landry

Mark Stalzer

Comment on my earlier posting on puncutation and spelling errors

Don Norman

Re: Caught with their pants down

Sean Malloy

Info on RISKS (comp.risks)

Gambling

Phil Agre <pagre@weber.ucsd.edu>

Sat, 19 Mar 1994 09:04:47 -0800

For those with an interest in risks, the technology supplement to Forbes magazine, Forbes ASAP, is a regular smorgasbord. The 10/25/93 issue, for example, includes an article about Bally's casinos' use of customer databases to optimize their investments in "comping", the practice of offering free drinks, hotel rooms, plane tickets, and what-not to high rollers. Given enough information about an individual's bets (regardless of whether they win), a straightforward economic calculation can decide which level of comping is optimal. (The full reference is: David H. Freedman, Odds man in [Bally's Atlantic City casino], Forbes ASAP, 25 October 1993, pages 33-35.)

The problem is getting the information into the computer. The Bally's casino accomplishes this in two ways. At roulette tables and the like, they simply have someone watch the game and enter bets into a portable computer. (This computer can also determine how much credit to extend to a given customer.) At the slot machines, they give each player a card with a magnetic strip that goes into the machine for as long as the player is playing. (They also offer a strap to keep the card attached to your wrist, so you don't walk away from the machine without it.)

The risks, of course, are obvious. Rational gamblers can take advantage of competition between casinos, choosing the best comping deal. But many people are addicted to gambling, and these innovations also make it easy for an addict on a binge to gamble away the maximum possible sum. Furthermore, as the article points out, "the riot of blinking lights, the clacking of spinning wheels, the absence of outside views or public phones -- all of this encourages the otherwise solidly grounded visitor to lose track of time and space, not to mention financial common sense". Profit margins are high, and investors are pleased.

The analogy to data-intensive marketing of cigarettes (see Risks 15.62) is strong. What's next? How about a frequent drinker's club for premium brands of liquor? Or individualized advice for children, based on detailed family demographics, about how to shame their parents into buying them expensive toys? It wouldn't be that hard. You could actually get a toy to do the explaining. Each product from a given toy company would contain a single chip with a small microprocessor, a simple RF receiver, some memory, and a speech synthesis device. When the toy goes through the checkout, an RF device built into the cash register downloads the toy with a demographic profile of the family derived from credit files pulled up through the purchase transaction. Then, as the child plays with the toy, the toy explains to the child the virtues of various other toys from the same company, along with suggestions for persuasion tactics that consumer research has shown to work well on parents in that particular market segment. If the toys can send as well as receive wireless data transmissions then newer toys can reprogram the older ones. Better yet, the child's videogame system, which will surely get its software over phone lines in the near future, could also download all of the child's other toys with new sales pitches, based on records of whether the previous pitches worked, as well as the latest market research and television and movie product tie-ins.

Phil Agre, UCSD

I really like this guy's attitude (Denver Baggage Handling)

"Alan (Miburi-san) Wexelblat" <wex@media.mit.edu> Mon, 21 Mar 94 11:51:55 -0500

[From EDUPAGE...]

- > Problems with an automated baggage-handling system controlled by 100
- > computers is delaying the opening of Denver's new airport. It's the first
- > such system to serve an entire airport, the first to be run by distributed
- > desktop computers, and the first to use radio links. Despite his woes, the
- > contractor says the project's worth it: "Who would turn down a \$193
- > million contract? You'd expect to have a little trouble for that kind of
- > money." (New York Times, 18 Mar 1994, C1)

Sure, he's getting his money -- what does he care if bugs prevent the airport from opening? I'd like to see the comments of the people who let the contract in the first place. On second thought, I probably wouldn't. It'd probably be the usual uninformed pablum about how complex systems "always" have a few "small" problems, and no thought given to how the problems might have been prevented in the first place.

Anyone want to bet they hire this same guy to do the upgrade when it's needed?

Feeling cynical on Monday morning...

--Alan Wexelblat, Reality Hacker, Author, and Cyberspace Bard, Media Lab - Advanced Human Interface Group wex@media.mit.edu Voice: 617-258-9168

Phone Machines Call Each Other, Part Deux

"Russell S. Aminzade: Trinity College of VT" <aminzade@moose.uvm.edu> Mon, 21 Mar 1994 12:28:53 -0500 (EST)

Several years ago, I posted an amusing story in this journal about two answering machines talking to each other. It was a choice enough RISKS tidbit to earn a place in Dunlop & Kling's Compterization and Controversy. I don't expect my 15 minutes of fame from this next one, but it seems I'm doomed to be the innocent witness while chatty answering machines interact with each other.

Imagine my surprise when I checked my answering machine at work and found a message which began "Hi, My name is [name]. I'm not at my desk, but if you'll..." Whoa! This was the voice-mail message of a friend. This friend works for a certain large, blue computer company which shall remain nameless:-)

I was certain this was the work of a prankster for a few reasons:

1) I don't know her direct-dial number. I've don't think I've ever called her at work, though I often talk with her husband who teaches at a nearby college.

2) We have an aging PBX. No direct-dial to me. Any call would have to be routed through our (very human) operator.

After a call to her to sic her company's phone-security cops on the perpetrator, and one to her husband (to play the message and prove I wasn't crazy) I had the weekend to ponder this odd event. I realized that it's entirely possible.

Here's how: Professor X calls my school, asks operator for my extension, gets answering machine, hangs up. He then calls his wife, gets voicemail, and hangs up. His college's switchboard, though, interprets the first hangup as a "flash," which means "forward this call to the next number I call"

The problem is a classical case of poor human-interface design -- the use of a switchhook flash to mean "transfer this call" when a slightly-longer flash means "hang up and give me new dialtone."

I can think of many grisly RISKs here, but for me the small but nagging one is that my friends may have jumped to the most obvious conclusion -- that I was the prankster.

Russell Aminzade: Academic Computing Coordinator, Trinity College of Vermont

[If it had been Pennsylvania, it would have been a PA de Deux. PGN]

✓ IRS Surveillance (Part II)

<Zajac@DOCKMASTER.NCSC.MIL> Mon, 21 Mar 94 01:22 EST

Recently, RISKS carried a posting on how the IRS was bidding for Dialed Number Recorders (DNRs) to record phone numbers.

The author suggested the IRS might be looking for a way to get the identity of individuals who call for information.

Readers should be aware that DNRs record the numbers that are called out on a target line. They are generally used only in criminal investigations.

If the IRS wanted to get caller information, they could do what large companies do today and get the caller ID (ANI) from each call that comes in on an 800 line. They would not have to go out and bid DNRs, the information is already available for free with their 800 number.

DOCKMASTER.NCSC.MIL

Dutch legislators trying to pull a fast one?

Ralph <ralph@runner.knoware.nl>

Tue, 22 Mar 94 15:07:37 GMT

Yesterday, leading Dutch newspaper 'De Volkskrant' reported that included into a new bill that deals with telecommunication, is an article that will outlaw cryptography in the Netherlands. One can apply for a waiver but they will want to know why you want to use cryptography, and they want your keys.

It looks like the Dutch government is trying to slip this one behind the backs of the voters just before the elections in may. Most stunning was that the Green party and others considered the issue 'a matter of little importance' and were not willing to do anything about it.

Lucklily the proposal is still in draft state, which means there is still time to get something done about it, but only if people are made aware of the consequences of such a law.

--Ralph Moonen --ralph@knoware.nl

Funny Money article in THE SCIENCES

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 20 Mar 94 21:05:47 EST

In "Funny Money" (_THE SCIENCES_ 34(2):6, March/April 1994), Brian Mono writes about counterfeiting using off-the shelf hardware and software. Nothing very new for RISKS readers, but it's a good one-page summary of the problem for novices. In brief:

- A report published in the autumn of 1993 by the National Research
 Council warns that the U.S. government has not kept up with technology used by amateurs to print counterfeit money.
- o Scanners, computers, colour printers and colour copiers [the distinctions among all of these devices are fading fast] tempt more people today to print small amounts of money.
- o Traditionally, counterfeiters have been few and concentrated in a few areas such as New York City. Casual counterfeiters are the opposite: many people over an enormous area.
- o In 1991, there were about 6-\$8 million of counterfeit money detected by officials in the U.S. (only 0.003% of the the Federal Reserve System's yearly total of 265 billion in currency handled).
- o "The dollar amount of scanned and color-copied fakes has doubled in each of the past three years...."
- o All countermeasures contemplated by the government must include consideration of backward compatibility: money-changing machines and business people have to be able to use both the older bills and whatever new ones appear.

- o Some recent countermeasures have had little effect; e.g., many bills have "so-called security threads, metallic polyester strips inscribed with USA and the denomination of the bill." Unfortunately, "hardly anyone outside the Treasury Department is aware of their existence."
- o Proposed countermeasures include colour-shifting ink and aliasing (a technique that tricks photographic reproduction machines into printing a line along the intersections of sets of parallel lines which are offset from each other at a particular angle). Holograms are also a practical possibility to deter amateurs.
- o One proposal from the NRC is that every copy machine print its serial numbers on every copy it produces. This technology is already in place in Xerox Corporation's "MajestiK" colour photocopiers. However, many observers are concerned about privacy issues. Norbert S. Baer, a member of the NRC committee, asked, "Would the Pentagon Papers have been leaked if identification numbers were implanted on them?"

[MK thinking out loud: AI pattern recognition algorithms coupled with a library of currency images could permit a smart copier to blank out all attempts to photocopy money. Such a technique would drive criminal hackers wild with the uncontrollable urge to crack the protection codes and actually make the poor machine _print_ the currency images. So the currency images would have to be one-way encrypted. But then the criminal hackers would try to decrypt the images. So there would have to be a cryptographically-sound checksum that could permit identification but not reproduction.

Comments?]

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Human Genome Project & Privacy

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 20 Mar 94 21:05:40 EST

A quick note to RISKS readers about a peripherally related subject--genetic counselling. This is a technique which far antedates computers, but today's Human Genome Project is heavily computer-dependent for data collection, analysis and storage of enormous amounts of information.

In a recent article (* see below), Robert Cook-Degan summarizes some of the problems we face with the growing ability to detect "bad" genes before birth as well as afterwards. Should everyone know about their own genetic defects? Always? Sometimes? What are the principles upon which to decide? Who should be allowed to know about _your_ personal genetic makeup? Do employers have a right to know that your family carries the gene for Huntington's chorea, which leads to uncontrollable movements and frank insanity in middle life? Do insurance companies have a right to reject an applicant for life insurance because of a family history of diabetes, breast cancer and alcoholism?

There's a section of the political debate between those who argue for abortion

of severely affected embryos (extremists argue for eugenic screening) versus those who argue for a more inclusive, accepting, less demanding society that can live with physical differences (extremists deny the existence of handicaps of any kind).

Interesting reading. It will be of special interest to those concerned about personal privacy in the computer age.

*Cook-Degan, Robert (1994). Private parts. _THE SCIENCES_ 34(2):18

Michel E. Kabay, Ph.D. / Director of Education, National Computer Security Association

✓ SGML--archiving style + content

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 20 Mar 94 21:05:51 EST

In _THE SCIENCES_ 34(2):4 (March/April 1994), Derek Coleman writes about the problem of interpreting machine-readable formatted text in archives. Technology changes so fast that an archive created a decade ago may be unreadable by programs running today.

Standard Generalized Markup Language (SGML). SGML includes standard English-language tags (e.g., <title>, <author>, <bold> and so on) that can easily by converted to any specific typesetting or word-processing system using a table-driven program (input string -> output string) or macro facility.

Using SGML, one converts today's text into standard ASCII. As long as the storage medium is physically readable (something that can be ensured by appropriate conversion over the years), SGML will permit a readable copy including enhancements to be prepared at any time on any platform.

Contact for more info:

International SGML users' group (U.K.) c/o Ms Gaynor West voice tel +44-793-512-515; fax +44-793-512-516

North America (Toronto):
Mr Yuri Rubinsky
voice tel 1-416-239-4801; fax 1-416-239-7105

Risk of bringing plastic cards through UK customs

Ross Anderson <Ross.Anderson@cl.cam.ac.uk> Sat, 19 Mar 94 14:01:09 +0000

UK customs officers have just been issued by the banking industry with magnetic card readers. The idea is that they will check suspects' plastic cards to make

sure that the magnetic strip details tie up with those embossed on the card face. This is reported in a recent issue of `Banking Technology'.

Not only are faults in magnetic strips fairly common, but poor maintenance of card readers has caused problems in the past. I have advised one man in the USA who is suing his bank after being arrested for altering the magnetic strip on his credit card. It turned out that he had not done this; the read head in the merchant terminal was probably misaligned, but in any case there was an alarm from the bank which the police took at face value. In the event, it took him about a year to slog through the banks' denials, get access to the card and have it tested by VISA to prove his innocence.

The risk to travellers is that some defect, whether in your card or in the customs man's reader, could get you arrested for fraud. If you are not resident in the UK, the courts might well refuse bail and keep you in jail for a year or more awaiting trial. If you are lucky, the Home Office might just deport you; but even this might be serious if you have relatives or other interests here.

Ross Anderson Cambridge University Computer Lab rja14@cl.cam.ac.uk

RISKs of safe ATMs

Sidney Markowitz <sidney@apple.com> Tue, 22 Mar 1994 16:51:48 -0800

I just saw a report of a press release from Dassault Automatismes Et Telecommunications, a French company that makes automated teller machines, about their new secure indoor lobby ATMs. The spokesperson is quoted:

"What a lot of people don't realize is that, if a thief tries to use a card which has been stolen, our ATMs are programmed to lock the doors and call the police. Not only is the customer secure from muggers, but the lobby ATM prevents card fraud,"

So if you use one of their cards, you had better hope that there are no data entry errors when a card with an account number similar to yours is reported stolen. And will a bank be careful to verify that it is really you calling to report your card as stolen and not someone who has decided to make trouble for you?

-- sidney markowitz <sidney@apple.com>

Re: Hard-drive headache!

David M. Miller <dmiller@hk.net> Wed, 23 Mar 94 00:42:12 HKT

I enjoyed the story told by Robert Telka (RISKS-15.65) but think there is more to be learned from this almost comical series of events than "you are never prepared enough". The RISKS are procedural rather than technical, but still related to IT.

The disk crashes caused Company P to be without IT services for several weeks. This surely cost them a tidy sum. Yet, recourse against the Plant Manager, who was the senior staff member on the scene, is limited as the "rule" he broke is unwritten. Should the manager be sacked, any lawyer worth their salt would make a good case for unfair dismissal. "Unwritten rules" can be broken as long as one doesn't do it in writing :-). The RISK is that staff members may not comply with the spirit. (They obviously can't comply with the text.)

Furthermore, the fact that both the primary and backup disks were in the same cabinet raises serious concerns about the contingency plans of the company. Contingency plans are often written for specific scenarios, when in practice nasty events such as these are never so neatly packaged. The RISK is that IT people are optimistic, causing them to underestimate threats, while Murphy is an absolute S.O.B. I would speculate that company IT management did not consider all aspects of a head crash -- obviously cabinet movement would be a likely cause....

IMO, the computer site should have been treated with more care and respect, since it was used by the sales force and other plants.

RISK: You lose your sales computer, maybe you lose your business.

David M Miller, GPO Box 4761, Central, Hong Kong dmiller@hk.net CompuServe: 100032,341 Fax: +852 987 1185

Copyright violations in RISKS Digest

Matthew B. Landry <mbl@ml7694a.leonard.american.edu> Fri, 18 Mar 94 20:28:24 EST

>I am absolutely not making this incident up; in fact I have it all on >videotape. The tape is from a local TV news show in Oregon, ...

The beginning of the quote saying "I am not making this up" tipped me off to begin with, but I read almost the whole thing before being positively sure that this message was in fact plagiarized from a humor column by Dave Barry. They even reprinted this column in one of his books.

Just thought people might like to know that this column is copyrighted by the Miami Herald and the author.

Matthew B. Landry, President of Project SAVE mbl@ml7694a.leonard.american.edu

[Similar comments also came from Ted Lemon <mellon@ncd.com>, straz@cambridge.apple.com (Steve Strassmann), danny burstein <dannyb@panix.com>, hoaglund@tecnet1.jcte.jcs.mil, Alan Bawden <Alan@lcs.mit.edu>, hartley@AIC.NRL.Navy.Mil, "Jonathan I. Kamens" <jik@cam.ov.com>. Marc Horowitz <marc@MIT.EDU>, "MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu>, mbraun@hydra.urbana.mcd.mot.com,

ROBINSON_PAUL@tandem.com, and I also got another posting of the Mahoney message from youngman@signal.dra.hmg.gb (neil youngman)! It is of course inevitable that some not-too-careful folks will pluck stuff off the net without including any source info. The problem compounds itself as the information moves along the net food chain. Stalzer's explanation follows. PGN]

Re: The RISKS of whale removal

<stalzer@macaw.hrl.hac.com>
Mon, 21 Mar 1994 08:55:34 +0800

I have been informed that most of the text of my posting was a Dave Berry column. The text was forwarded to me by a friend and, after laughing many minutes, I removed the headers to protect my friend's privacy and sent it off to risks in the hopes that everyone would get a good laugh. I apologize for any inconvenience. -- Mark

Comment on my earlier posting on puncutation and spelling errors

Don Norman <dnorman@apple.com> Mon, 14 Mar 1994 09:46:48 -0800

Commentary on my earlier note on punctuation and the resulting errors in spelling.

I have now received sufficient private and public messages to indicate that my knowledge of the history of punctuation and English orthography is seriously deficient: a clear example of the RISK that a little knowledge is a dangerous thing. So, please disregard my explanation of the origin of the confusion between the spelling of words of possession or that are contractions.

In my defense, however (the never-give-up defense), I still wish to argue that spelling errors are a result of what would amount to "poor design" were language and spelling actually designed.

the average speaker of English doesn't know the historical development of punctuation symbols or spelling and so is forced either to memorize apparently arbitrary and conflicting rules and examples or to construct a mental model that makes sense of the underlying structure. In my case, I constructed a mental model that has served me well in avoiding the common confusions among "its" and "it's." Alas, when I shared that model with you, the more scholarly among you were able to demolish its validity. This doesn't change the main thrust of the argument: were English punctuation and spelling designed with usability in mind rather than reflecting the complex evolutionary factors of its historical and technological development, we would have had less spelling confusions, especially of the its-it's variety. I'll back down and apologize about my scholarship, but not about the main point.

Don Norman, Apple Computer, dnorman@apple.com +1 408 862-5515 Apple Computer, Inc MS 301-3UE 1 Infinite Loop Cupertino, CA 95014 USA

★ Re: Caught with their pants down (Kabay, in RISKS-15.66)

Sean Malloy <malloy@nprdc.navy.mil> Sun, 20 Mar 94 14:52:09 PST

Animators have been putting 'easter eggs' like this into films almost since "Steamboat Willie"; it's an industry in-joke. In addition to the scene with Jessica Rabbit, there are also claims that a couple frames of the scene with Betty Boop were retouched, and that in the scene in the rest room, the phone number in the graffiti "For a good time, call Allisyn Wonderland XXX-XXXX" is the real phone number for one of the head animators.

In fact, I think that it may be that slipping a few frames like this into an animated production may have been easier when the shooting was all done by hand -- you just swapped a couple of reworked character cels for the regular ones while you're shooting a stack of cels onto film; when the tweening and coloring and 'cel' combination is all done electronically, there's more work involved in getting everything into the computer so you can tell it 'use _this_ set of character cels in frames X through Y instead of the pregenerated character cel sequence' without it being noticed.

In my opinion, anybody who takes this seriously deserves to.

Sean Malloy, Navy Personnel Research & Development Center, San Diego, CA 92152-7250 malloy@nprdc.navy.mil



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 69

Friday 25 March 1994

Contents

Another ATM failure (with a happier ending)

Mark Connolly

Bugs hold up farm cheques

Mich Kabay

Nut behind the wheel

Mich Kabay

Digital Telephone Switches and Modems

Bob Oesterlin

Grammatik bug mistaken for racial putdown

Marni Elci via Roy Beimuts

Re: Denver Baggage Handling

John Gersh

Marcus J Ranum

Bear Giles

Re: Funny Money article

Sean Eric Fagan

Curtis Jackson

Tobias Ulmer

Re: RISKs of safe ATMs

M. Hedlund

Re: Comment on earlier [Don Norman] posting

Marcus J Ranum

CFP: 2nd ACM Conference on Computer and Communications Security Li Gong

Info on RISKS (comp.risks)

Another ATM failure (with a happier ending)

Mark Connolly <connolly@hookup.net> Thu, 24 Mar 1994 08:22:14 -0500

Is there any interest in yet another ATM contribution? This one has all the familiar elements plus a reward for honesty to at least one of the participants (but not the other). Here are extracts from a newspaper story. [Mark Connolly, Connolly Design Inc., Waterloo, Ontario, Canada]

Bank machine runs amok; Honest customer returns bag full of cash SouthamStar Network

EDMONTON -- All Barry Inkster wanted when he slipped his bank card into the automated teller was \$200 to shop for a birthday gift for his wife. Instead he got a Las Vegas-style payoff when the machine spat out nearly \$5,000 in \$20 bills ... "I grabbed all the money in a great big wad and walked to a doughnut shop and asked them to give me a bag."... Inkster said he's been ripped off by automated tellers in the past, only to be told by bank personnel that machines don't make mistakes. ... the machine had been causing problems all weekend ... a number of people complained ... the machine was subtracting their withdrawals, but not handing out any money. ... No one from the bank was available for comment. A repair crew worked on the machine Monday morning but obviously it didn't fix all the problems ... Inkster called the bank, took the money back and watched the tellers count about \$4,800. ... "All I was concerned about was if the transaction had taken \$5,000 out of my account." The bank assured him it hadn't. Inkster said he was well rewarded with a pen, key chain and free dinner for his honesty.

✓ Bugs hold up farm cheques

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 23 Mar 94 09:15:44 EST

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe

Disaster Checks (By ROBERT GREENE, AP Farm Writer)

WASHINGTON (AP, 22 Mar 1994) -- The glitches stole Christmas from many Dade County, Fla., growers expecting disaster payments from the Agriculture Department. Because of processing errors, many checks for those who suffered losses in Hurricane Andrew have been held up for three months.

The author explains that about 5,000 cheques (a total of about \$25 million) were to have been mailed in December. However, staffers found serious errors such as a \$140,000 overpayment. As a result of procedural and computer bugs, "Of the \$24.8 million in payments, \$14 million has been reissued. And so far, \$1.8 million worth of payments has been canceled. Another \$11 million in payments remains on hold."

[It's bad enough to fight bugs in the fields without having to fight bugs in the banks.]

Michel E. Kabay, Director of Education, National Computer Security Association

Nut behind the wheel

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 23 Mar 94 09:15:48 EST

>From the United Press International newswire via Executive News Service (GO ENS) on CompuServe

Survey: few merchants check conflicting credit-card signatures written by Peg Byron, edited by Harold H. Martin, in New York

NEW YORK (UPI, 21 Mar 1994) -- Credit-card fraud may get an unintentional boost from retailers, Money magazine reported Monday in a survey that found 95 percent of clerks and cashiers they tested failed to check signatures on charged purchases. Money magazine said signatures for purchases that conflicted with the name on the credit card seldom caused clerks or cashiers to check for fraud.

The article continues with details of the experiment. Staffers used the wrong cards or signed false names in 127 cases (they had letters authorizing them to perform the experiment).

Only 5% of the store employees checked the signatures at all. "In one case, a male Money editor was not questioned even when he used a woman's card to charge a \$114 meal in a New York restaurant and signed the credit slip `Daffy Duck."

The cost of such fraud, entirely passed on to consumers, is about \$55 per card user in the U.S.

[Human factors control the effectiveness of security measures. We really do have to insist on PINs for credit cards.]

Michel E. Kabay, Director of Education, National Computer Security Association

Digital Telephone Switches and Modems

Bob Oesterlin <oester@vnet.IBM.COM> Fri, 25 Mar 1994 11:57:09 -0600 (CST)

Early last month, our local phone company (US West) replaced our "aging" analog telephone switch with a new digital one, which was designed to bring us "into the information age".

Well, no sooner was the switch installed, people started having problems connecting to our dial-in service for home terminal support. The current system consists of a front-end box (made by Traqnet) and a Cisco terminal server.

The problems seemed to be widespread but intermittent:

- Dropped connections
- Can't connect at 14.4 KB (drops back to 1200!)
- Can't connect at all

After some lengthy (and still ongoing) investigation, the problem turned out to be that the time bases of 3 digital switches involved are not in sync! The 3 are:

- The Rochester switch (run by US West)
- The IBM Rochester Local ROLM switch (local PBX)
- The NPN Switch (which connects IBM to the corp network run by Advantis, Inc)

Comments from our local communications rep:

"I have been told that there are 3 national master clocks. Each phone company must sync their digital switch with one of these master clocks."

"U.S. West's switch is sync'd with a master, I don't know which."

"NPN's switch is sync'd with a master too, this may be the same master that U.S. West is sync'ing to but, this is not important yet."

"Our ROLM switch is sync'd with NPN and cannot be changed."

BTW, the problem "seems" to be getting worse as time passes.

It would seem to me that this could become a widespread problem as more DSS's are used. Is someone causes a master clock to become out of step, then you could (potentially) disrupt communications over wide areas.

Bob Oesterlin, IBM AS/400 Division, Dept 54T, Rochester MN 55901 oester@vnet.ibm.com (IBM IPNET: oester@rchland.ibm.com) (507)-253-4528

Grammatik bug mistaken for racial putdown

"Roy Beimuts, Melfort Research Station, AGR CA" <BEIMUTSR@skrsme.agr.ca> 24 Mar 1994 15:27:50 -0500 (EST)

The following letter to the editor appeared in the March 23rd Globe and Mail; a very eloquent response to what must have been a very upsetting article.

Another illustration of how the most noble of programming intentions can backfire in the most unexpected ways due to an unforeseen bug:

Letter header: Software bug led to misunderstanding

I was distressed to read Mark Charendoff's essay Dear WordPerfect: I'm A Jew (Facts and Arguments -- March 8). Mr. Charendoff expressed dismay that Grammatik, WordPerfect's grammar and style checker, responded to the noun "Jew" with the message "Avoid this offensive term."

Mr. Charendoff's dismay is understandable. The message is absurd in that context. It was intended for "jew" used as a verb (e.g., "he jews

them down"). Grammatik's extensive dictionary contains two entries for "Jew"; one, capitalized, for the noun, and another, labelled "offensive," for the lower-case verb. When "Jew" or "Jews" occurs as the first word of a sentence, a bug in the program is calling the lower-case entry instead of the correct upper-case one. Ergo, the message is erroneously output.

The bug will be fixed. Its appearance in a program that I helped develop and am proud of is upsetting enough. That it resulted from our sincere efforts to identify and eliminate ethnic slurs troubles the whole Grammatik development team.

But other aspects of the situation disturb me personally as well. Please note that the opinions below are my own, not necessarily shared by WordPerfect Corp.

Mr. Charendoff remarks that many Jews he spoke with about this argued that "Jew" really is an offensive term. They tried to find some rationalization for the message. That troubles me. A word which identifies a whole heritage, a word as valid as "Protestant," "Buddhist," "Italian," or "Canadian," does not become offensive just because bigots use it, whether to demean or even to decimate. When Jews bend to that point of view, they reflect the confusion of a people that has survived oppression, only to be left with shame about its identity.

The automatic assumption by Mr. Charendoff and others that the message was an intentional racial putdown, not a mistake, bothers me too. Bugs occur often in software programs, especially those as complex as Grammatik. Parsing English is not easy. Granted, a bug involving one's religion may be hard to recognize as just an error. Although I wish he had written to us rather than The Globe and Mail, I cannot really blame Mr. Charendoff for his indignation.

Grammatik's goal has always been to help users find and fix problems in their writing. We think we have had good success so far, and we are constantly working to improve our performance. We are grateful that this mistake has been found so that we can correct it. But I would like the record to be clear -- this bug resulted from trying to eliminate prejudice, not propagate it.

Note: I come from a family of Orthodox Jews. Most of the members of my family who survived the Second World War now live in Toronto.

Marni Elci, English Linguist at WordPerfect Corp.
Albuquerque, N.M.

★ Re: Denver Baggage Handling (Alan Wexelblat, RISKS-15.68)

John R. Gersh <John_Gersh@aplmail.jhuapl.edu> Wed, 23 Mar 1994 15:38:17 -0500

It gets even more interesting...

The 7 Mar 1994 issue of *Aviation Week* has a story on the airport's yet-again-delayed opening. The hangup is indeed the complex automated baggage-handling system. The article says that the underlying problem is simply that system testing has not been completed in time, but it also describes some specific problems that have arisen. One is that:

"When United ran its tests, ticket counter agents were generating on-line printed baggage tags too rapidly, causing United's Apollo computer reservations system to communicate improper data to [the baggage system manufacturer's] baggage sorting computers. As a result, properly tagged luggage were being routed to a manual hold station instead of the aircraft, according to [the manufacturer's president]. 'It was mostly a training glitch,' he said. After the agents slowed down, the system operated nominally, he said."

While it's not entirely clear what "generating tags too rapidly" means here from the limited information given, one can envision various ways in which problems might arise. For those of us who spend all too much time in airport waiting lines, though, it's naturally disconcerting to hear that the system design requires the agents to work more slowly than they would like to!

It's even more disconcerting, however, to hear this described as a "training glitch," rather than a system design problem. My first reaction was to classify this as a typical case of blaming the user rather than the builder for problems in system design or implementation. Consider the following analogy, though: Airport check-in agents put luggage on a conveyor belt for dispatch to the baggage-handling area. Suppose there were a problem with agents "putting bags on the belt too rapidly" (i.e., piling bags on top of each other so that they fell off the belt or jammed the mechanism). Assuming that the belt speed was reasonably specified (based on other considerations), wouldn't it be proper to classify that as a training or procedural problem? Is that different from the overly-speedy tag printing?

Of course it is, and therein lies the key point. It's visually obvious what the proper placement of the bags on the belt should be; is it also obvious when the next acceptable tag-printing moment arrives? Suppose, only for the sake of argument, that other reasonable design constraints sometimes produce a significant communications delay between the two systems; that delay might result in the reservation system being able to print a baggage tag which the baggage system was not yet able to handle. In that case the real problem lies in not showing the agents that the overall system was not ready to print a tag or accept a bag. If, in fact, the agents can "generate tags too rapidly," then there is almost certainly something other than a "training glitch" at work. One might think either that the data generation or interchange timing is not as it should be or that the design of the agents' terminals does not adequately portray or control the effect of such possible timing problems.

John R. Gersh John_Gersh@aplmail.jhuapl.edu
The Johns Hopkins University Applied Physics Laboratory

Re: Denver Baggage Handling (Alan Wexelblat, RISKS-15.68)

Marcus J Ranum <mjr@tis.com>
23 Mar 1994 21:51:15 GMT

One thing that's particularly fascinating is that many of the problems they are facing (conveyor problems, zebra tags getting ripped and damaged, etc) are problems that Federal Express and UPS have apparently already solved.

I suppose UPS and Federal Express have the advantage that they can enforce packaging size limits and so forth, but it seems to me that one of the big RISKS we're seeing here is the ever-present danger of not doing your research.

Re: Denver Baggage Handling (Alan Wexelblat, RISKS-15.68)

Bear Giles <bear@tigger.cs.Colorado.EDU>
23 Mar 1994 20:07:42 GMT

You won't hear much griping from the politicians because *they* are the ones to blame for the delay. After the contract was signed, Denver kept asking for change after change to the luggage system. Nobody can develop a system on time and on budget if what they're developing keeps getting redefined!

On top of that, Denver made certain technical promises (e.g., a "clean" power supply) which it has been unable to fulfill. This directly lead to the failure of some of the early tests; a power surge would blow out circuitry, overrun motors, etc.

>It'd probably be the usual uninformed pablum about how complex systems >"always" have a few "small" problems, and no thought given to how the >problems might have been prevented in the first place.

It's pretty clear that Denver has a lot of airheads at the new airport. My favorite design flaw was the massive water sculpture directly over the main power transformers... requiring a large stainless steel catch basin.

Another good one (not directly related to the airport) was the initial proposal that one-way bus fare from Boulder to the airport would run about \$17. In contrast, the current bus fare from Boulder to Stapleton is about \$2.50. (The increase in distance would be about 30%). Toss in high taxi fares, and high car parking fees, and most people would choose to have a spouse or friend drop them off and pick them up. The impact on air quality is obvious.

Just remember, the mayor of Denver who pushed this monstrosity on us is now the Secretary of Transportation.

★ Re: Funny Money article in THE SCIENCES (Kabay, RISKS-15.68)

Sean Eric Fagan <sef@kithrup.com> Wed, 23 Mar 94 11:00:13 PST

>MK thinking out loud: Al pattern recognition algorithms coupled with a >library of currency images could permit a smart copier to blank out all >attempts to photocopy money.

It already exists. Xerox demonstrated it I think within the past year or two. When given money (both US and many non-US), it ignores it, and you end up with a blank spot on the paper.

The risks are obvious (to me, at least) and many.

★ Re: Funny Money article in THE SCIENCES (Kabay, RISKS-15.68)

Curtis Jackson <cjackson@mv.us.adobe.com> Wed, 23 Mar 94 12:35:04 PST

The new versions of the Canon Color Laser Copiers, the CLC 350 and CLC 550 (replacing the former CLC 300 and CLC 500) have exactly this type of protection built in, supposedly at the request (?demand?) of the U.S. government. I have no insight into the method used to prevent the copying of U.S. currency; I only know that the protection is in place in these products.

Curtis Jackson cjackson@mv.us.adobe.com or dod721@aol.com

★ Re: Funny Money (Mich Kabay, RISKS-15.68)

Tobias Ulmer <zccz1121@rpool1.rus.uni-stuttgart.de> Fri, 25 Mar 1994 13:04:27 +0100 (MEZ)

Such photocopiers are already in existence. I remember a demonstration in the German "Knoff-hoff" TV show (an entertainment show dealing with popular-science topics; and yes, the name is indeed derived from "know how") about one or two years ago. On the occasion of the introduction of new Deutsch-Mark bills at that time, the host explained the techniques that were used to make the bills counterfeit-proof. He finally concluded the discussion by taking a bank-note out of his wallet and laying it on a photocopier that he announced to be one of the latest inventions regarding the growing problem of counterfeit by use of those rapidly spreading color copiers. He pressed the button, not forgetting to mention smilingly that he was only allowed to do so because they had obtained a special permission and with police officers sitting in the first row of the audience, watching closely. What the machine produced was a verbatim copy of the bill but with colors changed to brilliant pop art. The host then showed a microchip that was the nucleus of the device that was said to recognize some dozens of bills from various currencies.

I would not expect such a chip to contain any such thing as protection codes to activate/deactivate the pattern recognition circuit, but instead a non-alterable read-only memory holding the images of the bills. So the difficulty isn't to protect the chip against being cracked but to prevent that its inhibiting output signal be disabled by means of a simple short cut. This can only be accomplished if some part of the system that is essential to the copying process is incorporated within that same microchip. The system has to be designed in such a manner that you cannot get the copier working without that chip so that it has the power to decide whether or not to copy. On the other hand, little can be done against a criminal attempt to replace the entire electronic control circuit board.

A more severe problem seems to be the fact that every once in a while new bills keep coming up which the device wouldn't yet be able to recognize. This requires that it is ensured that of every such existing copying machine the built-in firmware be updated (by replacing the chip with a newer version) every time when new notes are introduced with (at least) any of the leading currencies in the world.

Tobias Ulmer (zccz1121@rpool1.rus.uni-stuttgart.de) Student of Electrical Engineering

★ Re: RISKs of safe ATMs (Markowitz, RISKS-15.68)

M. Hedlund <hedlund@teleport.com> 23 Mar 1994 13:14:52 -0800

- > "[...] if a thief tries to use a card which has been stolen, our ATMs
- > are programmed to lock the doors and call the police. [...]"
- >So if you use one of their cards, you had better hope that there are no >data entry errors when a card with an account number similar to yours is >reported stolen. [...]

That's not all.....you'd also better hope: (1) you're not inside those doors when an actual thief tries to use a stolen card, not knowing or not caring about the "security" measures; (2) no natural nor manmade disasters occur while you're waiting for release; (3) the police know how to unlock the door; (4) your boss doesn't walk by the ATM atrium while you're stuck; (5) the bank installs a restroom (or at least, that you don't happen to need one); (6) the automated system succeeds in reaching the police and conveying your location; (7) the bank doesn't decide they're getting better use of your money while you're penned up.....

M. Hedlund <hedlund@teleport.com>

★ Re: Comment on earlier posting (Norman, RISKS-15.68)

Marcus J Ranum <mjr@tis.com> 23 Mar 1994 22:16:32 GMT

>In my defense, however (the never-give-up defense), I still wish to argue >that spelling errors are a result of what would amount to "poor design" >were language and spelling actually designed.

How can something that wasn't "designed" be an example of poor design?

Languages evolve (with exceptions like volapuk and esperanto) rather than being created from whole cloth by some rational process. Obsoleting a "living" language is a lot harder than fixing a programming language -- the installed base is potentially huge. Some legacy systems still actively communicate using Latin.

English, with all its commas and apostrophes and other bits of charm, is the result of a process of *translation* between the street English of the day and an approximation of written English. If I tried to write some of the

street speech from my neighborhood in ascii, it might look a lot like, "yo'm'a, cah yuh spa' me a qua'tuh?" Unlike compiled languages used by computers, spoken languages don't *NEED* to be designed and probably never will (the feelings of L'Academie Francaise aside).

Human minds are flexible enough to cope with the vagaries of "badly designed" languages. Spelling mistakes are a result of inattention to detail, ignorance, or apathy. The good news is that generally, the listener/reader will relatively painlessly absorb the error, rather than dumping core or giving a cryptic error like my compiler does when I forget punctuation.

✓ CFP: 2nd ACM Conference on Computer and Communications Security

Li Gong <gong@csl.sri.com> Fri, 25 Mar 94 15:11:20 -0800

Call for Papers

2nd ACM Conference on Computer and
Communications Security
Nov 2-4 1994
Fairfax, Virginia

Sponsored by: ACM SIGSAC, Hosted by: Bell Atlantic, George Mason University

High quality unpublished original research and practice papers in the area of computers and communications security are invited for consideration for the 2nd ACM Conference on Computer and Communications Security. All aspects of security are relevant, including:-

THEORY AND TECHNIQUES: Access Control, Cryptanalysis, Digital Signatures, Intrusion Detection, Audit, Cryptosystems, Formal Models, Randomness, Authentication, Cryptographic Protocols, Hash Functions, Viruses and Worms, Authorization, Database Security, Integrity, Zero Knowledge.

APPLICATIONS, CASE STUDIES & EXPERIENCES: Cellular and Wireless, LAN Security, Security APIs, Smart Cards, Electronic Commerce, Network Firewalls, Security Architectures, Telecommunications Security, Enterprise Security, Open Systems Security, Security Management, WAN Security.

SOCIAL AND POLICY ISSUES: Cryptographic standards, Information Privacy, Legal Issues, Technology Export.

PRACTICAL PAPERS DESCRIBING APPLICATIONS, CASE STUDIES OR EXPERIENCES ARE ESPECIALLY WELCOME.

INSTRUCTIONS FOR AUTHORS:

Format: FIVE copies of your paper (not to exceed 7500 words) in a form suitable for ANONYMOUS review (no author names, affiliations, obvious references, etc.) and a cover sheet with author name(s), address, phone and fax. Where possible all communications to authors will be via e-mail, so PLEASE PROVIDE an e-mail address.

SUBMIT TO: Prof. Ravi Sandhu, ISSE Dept., MS 4A4, George Mason University, Fairfax, VA 22030, USA (Ph#: 703-993-1659 E-Mail: sandhu@isse.gmu.edu) or Prof. Jacques Stern, ENS/ DMI, 45 rue d'Ulm, 75230-05 Paris, France (Ph# 1 44 32 20 29 E-Mail: stern@dmi.ens.fr).

Deadline: Papers must reach us by JUNE 1, 1994. Sorry, we cannot accept late submissions, and they will be returned unopened.

Authors will be notified of the Program Committee's decision by AUGUST 5, 1994, and will have to submit final camera ready papers by AUGUST 26, 1994.

GENERAL CHAIRS Dorothy Denning, Georgetown U and Raymond Pyle, Bell Atlantic

PROGRAM CHAIRS Ravi Ganesan, Bell Atlantic and Ravi Sandhu, George Mason U

TREASURER Richard Graveman, Bellcore

PUBLICITY CHAIR Li Gong, SRI

EUROPEAN CONTACT & PUBLICATIONS CHAIR Jacques Stern, ENS/DMI

PROGRAM COMMITTEE

Steve Bellovin, AT&T Eli Biham, Technion Joan Feigenbaum, AT&T Virgil Gligor, U of MD Li Gong, SRI Rich Graveman, Bellcore Sushil Jajodia, GMU John Kimmins, Bellcore Carl Landwehr, NRL Stewart Lee, U of Toronto David Maher, AT&T Roger Needham, Cambridge Clifford Neuman, USC ISI Paul Oorschott, BNR Bart Preneel, KUL P. Samarati, U of Milan Robert Shirey, MITRE Jacques Stern, ENS/DMI Byron Stump, Bell Atlantic Paul Syverson, NRL Bhavani Thuraisingham, MITRE Roger Tjarks, SAIC Michael Wiener, BNR Raphael Yahalom, Hebrew U



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 70

Monday 28 March 1994

Contents

April Fools on the Senate

John Dvorak and Chris Casey via Arthur R. McGee

Risks to government

Robert Davis

IRS persistence

Dave Methvin

BT Billing computers innocent

Marcus Marr

Insurance claims ignore patients name

David Bazell

The RISKs of Canadian Poodles using 911

John Oram

Ottawa, Canada, Radio contest overloads phone system

Henry Troup

911 as wrong number - they don't seem to care anymore

Jeff Hibbard

Re: Denver Baggage Handling

Jan Vorbrueggen

Re: The RISKS of whale removal

David G. Novick

Re: Banknotes and photocopiers

Tom Standage

Padgett Peterson

Info on RISKS (comp.risks)

April Fools on the Senate (fwd)

"Arthur R. McGee" <amcgee@netcom.com> Fri, 25 Mar 1994 19:50:47 -0800 (PST)

[PLEASE SEE MODERATOR'S NOTE BEFORE THE INCLUDED MESSAGE BELOW. THIS EXPLICITLY MARKED APRIL FOOL'S PIECE IS INCLUDED NOT FOR ITS SURPRISE VALUE, BUT IN THE PUBLIC INTEREST. PGN]

----- Forwarded message ------Date: Fri, 25 Mar 94 12:16:58 EST

From: Chris Casey@kennedy.senate.gov

To: ace-mg@esusda.gov

Subject: April Fools on the Senate

Hello ACE,

In the April issue of PC Computing, John Dvorak's column describes a Senate Bill, supposedly introduced by Senator Leahy and co-sponsored by Sen. Kennedy, to keep people from being intoxicated on the information highway. The column is an April Fools hoax and I'm sure plenty of people will find it amusing (see below).

Unfortunately there are also people that are actually believing it to be true. Our office has received several calls from outraged constituents and I understand Leahy's staff has as well. I originally received the article via e-mail, and I understand that the on-line rumors are flying leading some people to learn about it without the benefit of the actual article (which when read closely, reveals the hoax).

Congress has taken some great forwards steps recently, particularly through the availability of the Senate and House gophers (gopher.senate.gov, gopher.house.gov) and it would be unfortunate if people weren't aware of them. I share this with ACE in hopes that you can help quash any of these on-line rumors if you see them. Feel free to put people in touch with me if they'd like to hear more about what's happening in the cyber-Capitol:-)

Thanks for any help. I enjoy April Fools gags, but a lot of folks just aren't getting this one!

Regards,

Chris

Chris Casey chris_casey@kennedy.senate.gov
Office of Senator Kennedy 202/224-3570
Washington, DC 20510

[RISKS MODERATOR'S NOTE: THE FOLLOWING ITEM IS REPRODUCED IN THE RISKS FORUM WITH THE KIND PERMISSION OF THE AUTHOR, WHO HAS HIMSELF RECEIVED SEVERAL CALLS FROM PEOPLE WHO MISSED THE SPOOFINESS. John is quite well known for his annual spoofs. He noted to me that there are (at least) four clues herein. (See if you can find them, but don't bother informing RISKS.) As we approach the big day, I note that this piece is akin to the 1984 Chernenko spoof (due to Piet Beertema) and the "Spafford" spoof (due to Chuck von Rospach), the latter (see RISKS-6.52, 1 April 1988) fully laden with self-referential clues. PGN]

>Trust Congress? Not With This Unbelievable Lair of Slop

```
>PC Computing, April 1994, page 88.
>By John C. Dvorak
>
> When Vice President Gore began talking about the Information Highway,
> we all knew the bureaucrats would get involved more than we might
> like. In fact, it may already be too late to stop a horrible Senate
> bill from becoming law.
> The moniker -- Information Highway -- itself seems to be responsible
> for SB #040194. Introduced by Senator Patrick Leahy, it's designed to
> prohibit anyone from using a public computer network (Information
> Highway) while the computer user is intoxicated. I know how silly this
> sounds, but Congress apparently thinks that being drunk on a highway
> is bad no matter what kind of highway it is. The bill is expected to
> pass this month.
> There already are rampant arguments as to how this proposed law can
> possibly be enforced. The FBI hopes to use it as an excuse to do
> routing wiretaps on any computer if there is any evidence that the
> owner "uses or abuses alcohol and has access to a modem." Note how it
> slips in the word 'uses'. This means if you've been seen drinking one
> lone beer, you can have your line tapped.
> Because this law would be so difficult to enforce, police officials
> are drooling over the prospect of easily obtaining permits to do
> wiretaps. Ask enforcement officials in Washington and they'll tell you
> the proposed law is idiotic, but none will oppose it. Check the
> classified ads in the "Washington Post" and you'll find the FBI,
> National Security Agency, and something called the Online Enforcement
> Agency (when did they set that up?) all soliciting experts in phone
> technology, specifically wiretapping.
> It gets worse. The Congressional Record of February 19, 1994, has a
> report that outlines the use of computerized BBSes, Internet,
> Inter-Relay Chat, and CompuServe CB as "propagating illicit sexual
> encounters and meetings between couples -- any of whom are
> underage...Even people purporting to routinely have sex with animals
> are present on these systems to foster their odd beliefs on the
> public-at-large." A rider on SB #040194 makes it a felony to discuss
> sexual matters on any public-access network, including the Internet,
> America Online, and CompuServe.
> I wondered how private companies such as America Online can be
> considered public-access networks, so I called Senator Barbara
> Boxer's office and talked to an aide, a woman named Felicia. She said
> the use of promotional cards that give away a free hour or two of
> service constitutes public access. You know, like the ones found in the
> back of books or in modem boxes. She also told me most BBS systems
> fall under this proposed statute. When asked how they propose to
> enforce this law, she said it's not Congress's problem. "Enforcement
> works itself out over time," she said.
> The group fighting this moronic law is led by Jerome Bernstein of the
```

> Washington law firm of Bernstein, Bernstein and Knowles (the firm that first > took Ollie North as a client). I couldn't get in touch with any of the > co-sponsors of the bill (including Senator Ted Kennedy, if you can believe > it!), but Bernstein was glad to talk. "These people have no clue about the > Information Highway or what it does. The whole thing got started last > Christmas during an antidrinking campaign in the Washington D.C., metro > area," Bernstein said, "I'm convinced someone jokingly told Leahy's office > about drunk driving on the Information High and the idea snowballed. These > senators actually think there is a physical highway. Seriously, Senator Pat > Moynihan asked me if you needed a driving permit to 'drive' a modem on the > Information Highway! He has no clue what a modem is, and neither does the > rest of Congress." > According to Bernstein, the antisexual wording in the bill was > attributed to Kennedy's office. "Kennedy thought that technology was > leaving him behind, and he wanted to be perceived as more up-to-date > technologically. He also though this would make amends for his alleged > philandering." > > Unfortunately, the public is not much better informed than the > Senate. The Gallup Organization, at the behest of Congress, is > polling the public regarding intoxication while using a computer and > online "hot chatting." The results are chilling. More than half of the > public thinks that using a computer while intoxicated should be > illegal! The results of the sexuality poll are not available. But one > question, "Should a teenage boy be encouraged to pretend he is a girl > while chatting with another person online?" has civil rights activists > alarmed. According to Kevin Avril of the ACLU, "This activity doesn't > even qualify as virtual cross-dressing. Who cares about this stuff? > What are we going to do? Legislate an anti-boys-will-be-boys law? It > sets a bad precedent." > I could go on and on with quotes and complaints from people regarding > this bill. But most of the complaints are getting nowhere. Pressure > groups, such as one led by Baptist ministers from De Kalb County, > Georgia, are supporting the law with such vehemence that they've > managed to derail an effort by modem manufacturers (the biggest being > Georgia-based Hayes) to lobby against the law. "Who wants to come out > and support drunkenness and computer sex?" asked a congressman who > requested anonymity. > > So, except for Bernstein, Bernstein, and Knowles, and a few members of > the ACLU, there is nothing to stop this bill from becoming law. You > can register your protests with your congressperson or Ms. Lirpa Sloof > in the Senate Legislative Analysts Office. Her name spelled backward

Risks to government

Robert Davis <rdavis@nyx10.cs.du.edu> Mon, 28 Mar 94 16:20:48 GMT

> says it all.

My records show this happened on 22 February 1994.

The risks we take using computers are one thing, but the risks government officials take when talking about computers are extreme. Here I am, at home watching CSPAN. The entire morning is devoted to the new regulations from the Federal Communications Commission concerning cable television. I find it quite interesting. Then the chairman of the FCC shows up in a news conference. He answers questions about the new rules and regulations. The chairman of the FCC then opines that information about and from the FCC will appear on the "Information Superhighway". He says to connect to ftp.fcc.gov What follows is a near a quote as I remember his words: "G O V stands for government. FCC stands for [long pause] FCC. I don't know what FTP stands for." Remember, this is the chairman of the Federal Communications Commission speaking live on CSPAN. === Being a curious person, I made the connection to ftp.fcc.gov and as of that morning, no FCC files were available for FTP. However, one directory, bearing a name which may have been the initials of a system operator at the FTP site had something in it. One file, a GIF picture of actress Erika Eleniak, wearing most of her clothing, was available for FTP. So I grabbed it. As of today (28 March) that directory does not appear on the system, but there are directories containing FCC stuff.

rdavis@nyx.cs.du.edu Robert Davis Salina, KS

IRS persistence

Dave Methvin <0003122224@mcimail.com> Sun, 27 Mar 94 22:47 EST

Unlike [many others], I dutifully filed an IRS Form 942 for a nanny we employed in the first quarter of 1992. Unfortunately, my calculations were too high by a dollar; I suspect human error.

The ever-vigilant IRS computer found my mistake and issued a \$1.01 refund check within a month, even adding that penny for interest. Something about having a \$1.01 government check really tickled me, so I decided to just keep it instead of cashing it. Since the check expires after a year, I figured I was doing my part to reduce the deficit.

This week, two years later, I get _another_ check for \$1.01, with the same notation ("F-942 REF 03/92") as the previous check. I'm not cashing this one either; now I want to find out how badly they want to give me this money.

dwm

✗ BT Billing computers innocent

Marcus Marr <marr@dcs.ed.ac.uk> Mon, 28 Mar 94 13:50:39 BST

The current issue of New Scientist (26 March 1994, p. 19) includes an article following up from the one I quoted (<u>RISKS-15.56</u>, 17 February 1994: Telephone charges fail to fit the bill) regarding the overcharging on some telephone

bills in multiples of \pounds 420.

"Human error, not computer failure, was to blame for British Telecom's recent overcharging of some subscribers. BT says that each case of incorrect billing was caused by "an extremely unlikely combination of two human errors". The findings exonerate the computers, but indicate that BT staff sometimes ignore odd discrepancies in bills.

The first error arose when an engineer working on a new digital exchange broke house rules and used a procedure borrowed from old analogue exchanges. He sent a handwritten note to BT's billing department, asking it to log the meter reading as zero on its computer. The computer's software registers the last four digits of the meter reading, and on being given a reading ending in a string of zeros it deduced that the meter reading must have risen past 9,999 to 10,000. When the time came to prepare the bill, the computer then took the same logic a stage further and added together two spurious quantities: one from the last real reading up to 10,000, and one from zero to the new reading. Each unit costs 4.2p, leading to an overcharge of \pounds 420.

The second error came when BT's automatic verification system correctly highlighted these figures as inordinately high compared with past readings on the same line. But BT's staff ignored the warning and dispatched the bill, complete with errors."

New Scientist made no reference to their last sentence of the original article: ``[Insiders] believe that BT has a bug in its accounting software and that the problem is thus much more widespread than has so far been recognised.''

>From the article as I understand it, it seems that the computer software has difficulty in making the distinction between freshly reset meter readings, and normal 'clocked' meter readings. This could be explained cleanly if it was not possible (or unnecessary or difficult) to reset the meters of old analogue exchanges. The move to digital exchanges would therefore either need a change in the software or a change in the procedures. Ignoring my suppositions, though, the system (including personnel and computers) is designed correctly to cope with both analogue and digital exchanges.

Insurance claims ignore patients name

David Bazell

bazell@cuba.gsfc.nasa.gov>

Mon, 28 Mar 1994 09:58:33 -0500

I just got off the phone with my prescription plan holder, trying to find out why my son Jason's deductible had not been fulfilled. I picked up a prescription for him last week and had to pay the full \$43.95 cost of the medicine. My plan has a \$50 deductible per family member but I was sure that he had had several other prescriptions since the beginning of the plan year. I check my records and, sure enough, the prescriptions totaled more than \$50. After checking back with the pharmacy, it was determined that although the Jason's name was on the prescription, the prescription had gone toward

fulfilling my other son Graham's deductible. The pharmacist had entered the wrong code (02 rather than 03). However, I was also sure that Graham had had several prescriptions filled, so his deductible should already have been fulfilled. Further checking showed that Graham's prescriptions had been charged toward my deductible (my code is 00).

Talking to the prescription plan representative on the phone, I declared that this was a stupid way to do things. The system ignored the name that was entered and keyed only on the family member's number. I was assured that this was the best way to reduce the RISK of a mistake (he used that word). I guess the person who set up the system must have had several siblings with the same name.

Fortunately, my wife keeps all our medical records in good order so we were able to find documentation and figure out what had happened. The monitary cost to us would have been small if we had not sorted it out, but I can easily see this happening where the costs could be much higher.

Dave Bazell, General Sciences Corporation.

The RISKs of Canadian Poodles using 911

John Oram <oramy92@halcyon.com> Thu, 24 Mar 1994 22:44:12 -0800

VANCOUVER (Reuter) - A pesky pet played havoc with Canadian police who responded to an emergency call only to find they were barking up the wrong tree. A team of officers burst into a Vancouver home after receiving a 911 emergency phone call but found nothing more threatening than a poodle inside, police said Wednesday. The dog had knocked the phone off the hook and hit an automatic dial button that called police. Police feared the worst when all they heard on the line was the dog barking. "We came screeching over. It was a bit silly," confessed police spokesman Joe Arduini.

They had 911 on speed dial? Come on - that's inexcusable, given how easy it is to accidentally hit the wrong button on a phone. Do that many people die because they never finish dialing all three numbers? "Poor guy. Would have made it, but he was only able to hit 9-1."

I suppose the moral of this story is that the RISK isn't necessarily in the technology but rather in the people (mis)using it.

John Oram oramy92@halcyon.com

Ottawa, Canada, Radio contest overloads phone system

"henry (h.w.) troup" <hwt@bnr.ca> Mon, 28 Mar 1994 11:11:00 -0500

Friday, March 25th, the Ottawa radio station CHEZ-FM offered 53 pairs of Pink

Floyd concert tickets free to callers. The offer was open from 6 pm. The station is on a specially equipped exchange, but an estimated 300,000+ call attempts in an hour caused delayed dial tone and other problems from Cornwall, Ontario to Pembroke, Ontario (about 100+ miles). Ottawa is Canada's capital.

One story noted that some people (100 or so) called 911 to report telephone trouble, instead of 611. There were reports of actual outages, but it is not clear that people were waiting for dial tone and not hanging up and trying again.

Personal observation - I certainly had delayed dial tone, but only delayed 10 seconds or so.

One person I spoke to said that he had had seven phone lines active trying to get the free tickets.

Very little is new here. I leave the obvious pun for the moderator.

✓ 911 as wrong number - they don't seem to care anymore

Jeff Hibbard <jeff@bradley.bradley.edu> Mon, 28 Mar 1994 12:27:33 -0600

When 911 was first implemented (many years ago) here in Peoria IL, everyone with a phone number of the form x91-1xxx was forced to change their numbers.

After a few years, though, the phone company started reassigning numbers of this form.

Jeff Hibbard jeff@bradley.bradley.edu

[In various old small-town switching centers, one could dial just the last four digits, or in some cases five digits, for local calls. That led to similar problems when 911 was introduced, and has now disappeared almost everywhere in the U.S.A. (although for other reasons as well.) PGN]

Re: Denver Baggage Handling (Wexelblat, RISKS-15.68)

Jan Vorbrueggen <jan@neuroinformatik.ruhr-uni-bochum.de> 25 Mar 94 12:41:34 GMT

- 1. I would think Frankfurt/Main airport (FRA) was the first to have an integrated, computer-controlled baggage distribution system. For years I heard they were the only international airport able to guarantee 45 minute connections because of it.
- 2. When the system was installed (ca. '72), the contractor, AEG, required something like six months past the deadline to get it running. In that time, they reputably paid a penalty (or whatever you call "Konventionalstrafe" in English) of DM 200K _per_day_. I don't think they made much profit on the contract...

Jan

★ Re: The RISKS of whale removal (Stalzer, RISKS-15.67)

David G. Novick <novick@cse.ogi.edu> Mon, 28 Mar 94 10:02 PST

I cannot explain why the Highway Dept. chose to blow up the deceased whale. I can, however, explain why this problem fell to the Highway Dept. Unlike most states, which allow private ownership of beaches, Oregon has kept all its beaches owned by the state. The mechanism for this, curiously, is that the beach is technically part of the of state highway system--although you generally aren't allowed to drive on it. So the whale shows up on a state highway, and it's the Highway Dept.'s problem

David G. Novick | Department of Computer Science and Engineering | Oregon Graduate Institute of Science & Technology novick@cse.ogi.edu | 20000 N.W. Walker Road tel (503) 690-1156 | P.O. Box 91000 fax (503) 690-1548 | Portland, OR 97291-1000

Are there really pictures of banknotes inside photocopiers?

Tom Standage <thomas@primrose.demon.co.uk> Mon, 28 Mar 94 13:49:47 -0800

Following the resent posting about how photocopiers prevent banknote forgery, I wonder how many other readers' jaws dropped open at the suggestion that there is a ROM inside a colour photocopier (such as the Canon CLC350/550) with images of common banknotes in it. This just wouldn't make sense, aside from the fact that it would rapidly go out of date - it would simply be too computationally expensive to compare every image placed on the copier with the images in ROM. The Canon machines in question can also be used as colour laser printers in conjunction with special interfaces, so presumably any anti-forgery computer inside the copier would also have to check that banknotes weren't being scanned into a personal computer and then printed out via the colour copier. This is absurd.

We have a CLC300 at work, and when an engineer came to fix it one day, he said that the problems we were having (with jammed paper) were a design fault that had been fixed on the CLC350. I asked what other features the 350 had, and he said it had anti-forgery features - and proceeded to tell me the same story about a chip with pictures of banknotes in it. I found this so hard to believe that I asked around, and eventually someone gave me a more believable explanation. Apparently the security measures depend on special inks used when the banknotes are printed. These inks change colour when illuminated by the scanner in the copier, and produce copies of the banknote with an obvious colour shift. I don't know whether the 350 and 550 have a different kind of bulb in the scanner or are able detect the special inks, but I have also heard of other documents that won't copy properly because the copier thinks they're

banknotes. Rumour has it you can get round this by photocopying through very thin tracing paper - which presumably works with banknotes as well.

Anyhow, perhaps someone at Canon can give us a definitive answer. On the other hand, I wouldn't be surprised if they wished the status quo to continue, where we all believe that copiers have chips with pictures of banknotes in them. What makes me laugh is the message on the front panel of the CLC300, which warns you not to copy money or certain other documents: "you *may* be committing a criminal offense for which you *may* be prosecuted." Pretty strong language, huh?

"Funny Money" and Smart Copiers

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Fri, 25 Mar 94 19:58:12 -0500

Once upon a time, long long ago in a galaxy far far away, an automobile manufacturer known to all of its employees as "Generous Mother" began using computers to control such things as mixture and spark advance and a host of other variables. The maps for these variables were carried in 1k x 8 PROMS.

Certain individuals who shall remain nameless acquired the maps of these programs for certain "performance" cars and designed their own maps.

Unfortunately, these new maps, though amazing in improving performance and efficiency were not what the manufacturer had certified.

So the aspiring young engineers replaced the 1k x 8 PROM with a 2k x 8 EEPROM and a switch concealed under the dashboard. The lower 1k contained the stock settings and the upper 1k, settings of a more "interesting" variety. For roadside tests the switch was turned "off" and for normal driving "on".

I suspect that copiers that rely on "firmware" to block copying of bills might soon acquire such switches.

Padgett

[RISKS received lots of mail on this topic, most of which is NOT included, including bob@demosthenes.ilt.tc.columbia.edu (Bob Matsuoka), dgursky@nextsrv1.andi.org (David Gursky), jml4@cus.cam.ac.uk (John Line), hoover@cs.ualberta.ca (Jim Hoover).

dylan@mundil.cs.mu.OZ.AU (Dylan John SHUTTLEWORTH) noted that Australian \$5 and \$10 notes are plastic with a transparent "hole" around a hologram. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 71

Tuesday 29 March 1994

Contents

Risks of washroom automation

Paul Colley

Pav-per-View failure lets adult station go unscrambled

Mike Carleton

Role-playing Addiction

Mich Kabay

Software theft statistics

Mich Kabay

Risks of spelling checkers

John Girard

PGN

Busy-waiting woes

Darren Senn

Recent useful newspaper pieces on crypto policy

Lance J. Hoffman

Re: L.A. Phone Fire

Nevin Liber

Re: Canadian Poodles using 911

Shawn Mamros

Re: Banknotes and photocopiers

Mike Sullivan

Re: IRS persistence

Robin Kenny

Preliminary Program: 7th IEEE Computer Security Foundations Workshop

Li Gong

Info on RISKS (comp.risks)

Risks of washroom automation (Erma Bombeck)

<ember!pacolley@qucis.queensu.ca> Mon Mar 28 14:22:02 1994

Here's one paragraph of Erma Bombeck's humour column, The Kingston Whig-Standard, 28 March 1994.

"I dropped by an airport washroom. In my stall, I wrestled with my jumpsuit, and in doing so the belt fell into the commode. Before I could retrieve it, the automatic flusher sucked it away and into the sewers of San Jose. I held my hands under the automatic water tap and went for a paper towel. I turned in time to see my handbag fall into the sink and activate the water. It proceeded to drown."

The column also enumerates many other more familiar problems with automation.

- Paul Colley colley@qucis.queensu.ca +1 613 545 3807

[Beware of the automatic handwringer. PGN]

Pay-per-View failure lets adult station go unscrambled

<mcarleton@zendia.enet.dec.com>
Tue, 29 Mar 94 13:37:20 EST

Cable company adds unexpected Spice to subscriber's dinner hour.

A problem with a pay-per-view system caused all customers of the Greater Media Cable TV service in Worcester Massachusetts to receive the unscrambled broadcast of an Adult cable cannel offered by the system. The Spice cable channel was unscrambled for 90 minutes between 6:00pm and 7:30pm on Monday March 28th.

According to a representative of the cable company, Ed Goldstien, the cause of the glitch was not known and an investigation was in progress.

Goldstien presented the cable company's apology and promise that it would not happen again to subscribers over the local radio station WXLO.

The Greater Media Cable system uses a call in voice response system to allow customers to activate the pay-per-view stations offered by the system. The activation code for the customer's cable box is broadcast over the cable system to unscramble the selected pay-per-view offering. RISKS readers could speculate that this incident is an indication that a universal activation code must exist for all cable decoders in the system. We could further speculate that the voice response system could have broadcast this code in response to a pay-per-view request of a single subscriber if internal tables were faulty.

The RISK here is dependence on an automatic system to save cost when the cost of its failure is not taken into account.

Mike Carleton mcarleton@zendia.enet.dec.com

Role-playing Addiction

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 29 Mar 94 12:59:07 EST

Washington Post Staff Writer John Schwartz has published a moving and insightful article entitled, "Game Boy." It explores the life and death of an eighteen year old man addicted to cyberspace role-playing. I have asked Mr Schwartz for permission to post the original article in its entirety. For the time being, here's a brief summary.

<<

Software theft statistics

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 29 Mar 94 12:59:16 EST

>From the Associated Press newswire via Executive News Service on CompuServe (GO ENS):

JEANNINE AVERSA, Associated Press Writer, reports on the Software Publishers Association's statistics concerning software theft. Key findings:

- o Worldwide losses of \$7.4 billion for business software in 1993.
- o Rate is down 25% from \$9.7 billion in 1992.
- o Business software (spreadsheets, electronic mail, accounting and data base programs) sales revenues in 1993 were \$6.8 billion.
- Companies whose employees make unauthorized copies or put single-copy programs on network servers account for the most frequent violations of software copyright.
- o The SPA audited or initiated lawsuits against 245 companies, all of which were resolved out of court.
- o Settlements totalled \$3 million.
- o Manufacturers in the U.S. lost \$1.57 billion; Japan lost \$650 million; France lost \$435 million.
- o Software theft grew fastest in India and Pakistan (up 95%); Korea and Brazil showed 89%, and Malaysia's theft grew 88%.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

✓ Risks of spelling checkers

John Girard <jgirard@cix.compulink.co.uk> Tue, 29 Mar 94 23:32 BST-1

I was recently quite shocked (UK: gob-smacked) to find that an event

connected with my spell checker could have put me at risk of losing my job. I was editing a publication to be sent to several hundred of my client contacts, and had made a series of trivial spelling corrections, the last being a "replace". Sitting poised over the replace button, I was presented with the suggestion that the word "Goldman" (as in a large company we all know) should be replaced with "goddamn". The word processor involved was MS Word for the Macintosh. I then tested this on Word for Windows, and got the same result. (I have the `always suggest' option selected)

This event scared me greatly, because it is easy to go unconscious in front of the mouse and press "replace" one too many times without realizing the result. I contacted my support agency and was told that "goddamn" is in the main dictionary, and that I could not delete it from the main dictionary. It was suggested that I program Goldman as a replacement to goddamn.

Of course, defining a replacement in this one case does not assure me that the "bad" word will not be suggested in the future for other replacements. And, I have not yet encountered other unprofessional and undesirable word replacements which I would grudgingly agree that, in an academic sense, belong in the dictionary, but are a risk to my job. Yet, I wait in fear of these discoveries.

My concern here is that products such as word processors that are sold for use in "business" applications should either not freely suggest profane words in the main dictionary, or should have an option to leave them out or supply an extra warning. Obviously, the problem is further complicated by words or phrases that have different meanings in different countries even when the language seems otherwise equivalent.

Has anyone else had problems similar to this? Are there any alternative "business-oriented" main dictionaries which can be purchased to eliminate the risk? And, should I be obligated to live-with/fix this problem when purchasing a "business" product?

John Girard New Science Associates, Ltd./ UK

★ Re: Risks of spelling checkers (Girard, RISKS-15.71)

"Peter G. Neumann" < neumann@csl.sri.com> Tue, 28 Mar 94 16:21:07 PST

The RISKS archives are full of cases such as transforming a Mafia "enforcer" into an "informer", "payout" into "peyote", "back in the black" to "back in the AfroAmerican", and many other garbles. And I just happen to notice a note from Abhijit Chaudhari <abhijit@sware.com> in the YUCKS digest (from spaf@cs.purdue.edu) noting that NeXTSTEP 3.0 Webster's barfs on "UNIX", and offers "unfix" instead. That is not Unix-friendly, although I distinctly recall Steve Jobs suggesting at the San Francisco birth announcement for NeXT that NeXT was UNIX-emulatable and UNIX-friendly (but that nobody would care once they had seen NeXT!). I wonder what that spelling corrector does to NeXT? Maybe it gets turned into a NeWT.

Busy-waiting woes

Darren Senn <sinster@scintilla.santa-clara.ca.us> Tue, 29 Mar 1994 00:19:48 -0800 (PST)

A few years back, I was working as a student computer consultant at UC Santa Cruz. The San Diego Supercomputer Center was pulling itself up by its bootstraps, and a few of the researchers at UCSC had won grants of CPU time on SDSC's CRAY Y/MP.

SDSC sent some of their tech. support staff up to Santa Cruz to give our researchers a quick introduction to UNICOS (CRAY's flavor of SYSV UNIX) and SDSC's special features. Needless to say, they didn't want to leave their tech support people in Santa Cruz, so they gave us a small grant for our consultants to use while learning their system. I was one of the lucky consultants who got to participate.

So far so good.

At the same time, one of my friends was finishing up his physics thesis (a weird little study of aerodynamic surfaces), and had written a small flight simulator to do some of his calculations. This study was weird enough that my friend was calling his programs 'funny', 'goofy', 'damgoofy', etc. It was a simple program which simulated the flight of a plane for a short duration, and the user couldn't adjust any control surfaces after the program started.

As a favor to him and as a convenient way to learn more about the Y/MP, I ported his program over to UNICOS.

The program normally asked the user for its parameters when it started up, printed the results to the terminal, and waited for the user to hit return before quitting. The program was almost entirely math, so all I had to do was convert it to batch processing. Simple: just change a few scanf()'s to fscanf()'s, tweak a few paths, and we're all set.... Or so I thought. (ominous background music, please).

I ftp'd the files over to the cray, compiled them, and made a few short test runs. No problems. So I set it up to calculate 30 seconds of flight at 1ms intervals, and to print out the time when it started and stopped. Then I set it loose. It was truly impressive watching those columns of numbers scrolling by. But alas, my next class was starting, so I couldn't wait for it to finish. I was capturing the output to a file anyway, so I just disconnected and went to my class.

That was Friday evening.

Sunday morning rolls around, and I get rudely shaken from bed by a phone call at 7am! Imagine the nerve! hmph. It was SDSC's support staff calling. It seems that a renegade program had eaten up all the consultant's time grant by running continuously (100% CPU usage) for 35 hours in the interactive 'batch' queue! Clearly this program was intended as some warped prank, considering it was called 'damgoofy'! Uh-oh. I was sure there was some kind of mistake, so I rushed up to campus to see what had happened.

It turns out that I had forgotten to remove the program's last gets(): that's the line which made the simulator wait for the user to hit return before quitting. That shouldn't have been a problem in itself, since the function should've immediately returned with an error after it discovered it had lost it's terminal (when I logged out). It didn't. No problem, right? The program should've just stopped waiting for input, consuming no CPU resources. Nope. Under that version of UNICOS, the program was waiting in a busy-loop, uselessly using the CPU while it waited for input. :(Ooooops!

Luckily SDSC was nice to us, and the Y/MP was underutilized back then anyway, so they just refunded the money, my friend got an impressive simulation, and I got an anecdote. :)

Darren Senn Phone: (408) 988-2640 Snail: 620 Park View Drive #206 sinster@scintilla.santa-clara.ca.us Santa Clara, CA 95054

Recent useful newspaper pieces on crypto policy

"Lance J. Hoffman" <hoffman@seas.gwu.edu> Tue, 29 Mar 1994 14:01:51 -0500 (EST)

Two interesting newspaper articles on encryption policy recently appeared:

In The Australian, an influential national newspaper similar to The Guardian in the U. K. or The New York Times in the U. S., a large article describes the Clipper chip controversy including a bit more technical detail than is common for U. S. newspapers. Professor Bill Caelli of Queensland University of Technology's School of Data Communications is quoted as saying "Is Clipper the start of a more onerous agenda? Does Clipper represent attempts to outlaw the use of encryption in any form by the public unless he or she uses an 'approved' (and breakable) cipher system such as Clipper? This last question is a far darker scenario and goes to the very heart of freedom and privacy in a democratic society." -- All this in The Australian of 29 March 1994.

In the New York Times of 26 March 1994, on the first page of the second section and wrapping around to page 26, there is an article "Collisions in Cyberspace on Data Encryption Plan" which starts "To paraphrase Oscar Wilde, the Clinton Administration threw a couple of its lions into a den of savage Daniels here this week" (now last week). That refers to the Fourth Conference on Computers, Freedom, and Privacy in Chicago, and the article appears under a wonderful photo of Emmanuel Goldstein, editor of 2600, clad in T-shirt, etc., taling with Frank Carey of Bell Labs, replete in coat and tie, but holding beer bottle. The article goes on to describe an arrest of a man in the conference hotel (actually a conference attendee) who fit the description of fugitive hacker Kevin Mitnick and the rough go Dave Lytel of the President's Office of Science and Technology Policy had as the keynote speaker trying to defend Clipper.

Professor Lance J. Hoffman, Department of Electrical Eng. and Computer Science The George Washington University, Washington, D. C. 20052 (202) 994-4955

★ Re: L.A. Phone Fire (Weinstein, RISKS-15.67)

Nevin Liber <nevin@cs.arizona.edu> Tue, 29 Mar 1994 02:32:49 -0700 (MST)

We felt the effects here in Tuscon, Arizona, 500 miles and another state away from Los Angeles. I went to the local grocery store to do some shopping and, you guessed it, they couldn't take my charge card because of that fire (they had notices posted throughout the store).

I guess it's not just earthquakes anymore that have a rippling effect all the way to Arizona...

★ Re: The RISKs of Canadian Poodles using 911 (RISKS 15.70)

Shawn Mamros <mamros@ftp.com> Tue, 29 Mar 94 10:55:27 EST

John Oram <oramy92@halcyon.com>, in RISKS 15.70: >They had 911 on speed dial? Come on - that's inexcusable, given how easy it >is to accidentally hit the wrong button on a phone.

Not when the phone manufacturer provides speed dial buttons explicitly labelled for that purpose. I own a General Electric phone (purchased about five years ago) that has three buttons on it labelled "Fire", "Police", and "Ambulance".

There are other risks associated with such a phone, in addition to that of pets (or small children) accidentally hitting one of those buttons. The buttons need to be programmed with the correct number, since 911 is not (yet) universal in the US. If the owner of a phone does not set the numbers for those buttons - or worse, moves without changing the numbers (where one of the old or new locations does not have 911) - one could picture a scenario where a guest is present, the phone's owner is incapacitated, and the guest tries to use the "Ambulance" button to contact same...

-Shawn Mamros mamros@ftp.com

[RISKS received a large number of messages on this topic, including those
Jay Schmidgall <jay@VNET.IBM.COM>,
Jeff Nelson <jnelson@gauche.zko.dec.com>,
Nevin Liber <nevin@cs.arizona.edu>,
Tom Russ <tar@ISI.EDU>)
Andrew Duane <duane@zk3.dec.com>
who noted built-in emergency features. The risks therein seem quite
widespread. Also,
Bob Peterson
peterson@choctaw.csc.ti.com>
noted the risks of defaults returning when batteries are replaced. PGN]

Banknotes and photocopiers

Mike Sullivan <74160.1134@CompuServe.COM> 29 Mar 94 00:12:24 EST

In RISKS-15.70, Tom Standage noted that some color photocopiers prevent forgery by reacting to the color shift in the ink. This seems similar to how our Xerox black-and-white copiers react to an American Express card. The cards apparently use two different inks for the pattern filling the face of the card, one of which is invisible to the copier, although both inks look identical to the eye. When photocopied, the card image bears the word VOID all over its face (this is the green card; haven't tried it with a gold or platinum one). Perhaps a similar technology is involved in preventing copying of currency.

★ Re: IRS persistence (Methvin, RISKS-15.70)

Robin Kenny <robink@hatchet.aus.hp.com> Wed, 30 Mar 94 10:16:25 +1000

This is not a good idea. What happened to me, basically, was that I closed my old VISA account with the State Bank Victoria (Australia) with 4 cents credit, <CREDIT, not debit>, believing I was a good guy for not trying to get the money out - after all, it probably costs VISA \$x per transaction. Some years later I had occasion to apply for another VISA card...

When trying to use my bank DEBIT card to pay for petrol a security alert was flashed to the operator and my card was seized. Using my ATM card showed no funds and my ATM card was seized. My PASSBOOK account had a security trigger fire when I presented it at the local branch... It was all caused by the previous VISA account; the four cents was never allowed to be reabsorbed by the bank and my application for a new card found a bug in the validation software that said "there is a problem with this applicant". This automatically put a hold on all my finances! Even the home loan joint account was frozen. It took TEN WORKING DAYS for a human to finally backtrack to the root cause (the security re-asserted itself each night) I did get an official letter of explanation (I was beyond accepting apologies) on letter-head so future repercussions could be minimised.

What may happen to "dwm" could be something bizarre like being arrested by the IRS for undisclosed income, not so improbable as a friend had his 1987 tax refund assessed as income for 1988!

(Did I read in RISKS about a person having \$1M accidentally transferred into their savings account, now fighting it out with the bank over the \$50,000 funds-transfer tax?)

[The original item was in <u>RISKS-15.60</u>. I don't recall seeing the transfer-tax item before. PGN]

Robin Kenny (robink@hparc0.aus.hp.com)

Preliminary Program: 7th IEEE Computer Security Foundations Workshop

Li Gong <gong@csl.sri.com> Tue, 29 Mar 94 10:33:56 -0800

[This workshop is by invitation of the General Chair only. To participate, please contact Professor Ravi Sandhu at sandhu@isse.gmu.edu as early as possible since the number of spaces is very limited.]

7th IEEE Computer Security Foundations Workshop (CSFW-7) (Preliminary Program) Franconia, New Hampshire, June 14-16, 1994

Tuesday, June 14

8:50-9:00am -- Welcoming Remarks
Ravi Sandhu (George Mason University, General Chair)
Li Gong (SRI, Program Chair)

9:00-10:30am -- Non-Interference and Composability Session chair: Jose Meseguer (SRI)

- * Unwinding Forward Correctability
 Jonathan Millen (MITRE)
- * A State-Based Approach to Non-Interference
 William Young and William Bevier (Computational Logic, Inc.)
- * Combining Components and Policies
 George Dinolt, Lee Benzinger and Mark Yatabe (Loral)

11:00-12:00pm -- Formal Methods and Semantics Session chair: Simon Foley (University College Cork)

- * Formal Methods for the Informal World
 Carol Muehrcke (Secure Computing Corporation)
- * Formal Semantics of Rights and Confidentiality in Deductive Databases with General Integrity Constraints Adrian Spalka (University of Bonn)

12:00-2:00pm -- Lunch Break and Croquet Tournament

2:00-3:00pm -- Modeling
Session chair: Stewart Lee (University of Toronto)

- * Confidentiality in a Replicated Architecture Trusted Database System:

 A Formal Model

 Oliver Costich, John McLean and John McDermott (Naval Research Lab)
- * Conceptual Foundations for a Model of Task-based Authorizations Ravi Sandhu and Roshan Thomas (George Mason University)

3:30-5:00pm -- Panel on "The General Write-Up Problem"
Panel moderator: John McDermott (Naval Research Lab)

Panelists: to be confirmed

Wensdesday, June 15

9:00-10:30am -- Cryptographic Protocol Analysis Session chair: Virgil Gligor (University of Maryland)

- * A Model of Computation for the NRL Protocol Analyzer Catherine Meadows (Naval Research Lab)
- * AUTLOG -- An Advanced Logic of Authentication Volker Kessler and Gabriele Riemer (Siemens, AG)
- * Nonmonotonic Cryptographic Protocols

 Aviel Rubin and Peter Honeyman (University of Michigan)

11:00-12:00pm -- Security Policies

Session chair: John McLean (Naval Research Lab)

- * Formal Specification of Information Flow Security Policies and Their Enforcement in Security Critical Systems
 Ramesh Peri and William Wulf (University of Virginia)
- * A Taxonomy of Security Properties for CCS Roberto Gorrieri and Riccardo Focardi (Universita di Bologna)

12:00-2:00pm -- Lunch Break and Croquet Tournament

2:00-3:00pm -- Access Control

Session chair: Joshua Guttman (MITRE)

* One-Representative Safety Analysis in the Non-Monotonic Transform Model

Ravi Sandhu and Paul Ammann (George Mason University)

- * Reasoning about Confidentiality Requirements Simon Foley (University College Cork, Ireland)
- 3:30-5:00pm -- Panel on "Reconsidering the Role of the Reference Monitor"
- * Redrawing the Security Perimeter of a Trusted System

 Dan Sterne and Glen Benson (Trusted Information Systems)

Panel moderator: Dan Sterne

Panelists: Len LaPadula (MITRE), Ravi Sandhu (GMU), Carl Landwehr (NRL), and Glenn Benson (TIS)

Thursday, June 16

9:00-10:30am -- Protocol Security

Session chair: Michael Merritt (AT&T Bell Labs)

- * Development of Authentication Protocols: Some Misconceptions and a New Approach Wenbo Mao and Colin Boyd (University of Manchester)
- * A Taxonomy of Replay Attacks Paul Syverson (Naval Research Lab)
- * Cryptographic Protocols Flaws
 Ulf Carlsen (Telecom Bretagne, France)

11:00-12:00pm -- Workshop Business Meeting

12:00pm -- Workshop Adjourns



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 72

Thursday 31 March 1994

Contents

Mud Slide Cuts East Coast Phones

PGN

Briton Survives "Monster" Attack due to computer glitch

Will Deatrick

Risk Evasion Measures Create New Risks

Stephen A. Stough

Rental cars and financial derivatives

Phil Agre

White collar crime in Australia

Mich Kabay

Hotline reassignment

Mich Kabay

Electronic purse

Mich Kabay

Dials!

Bob Frankston

Re: Spelling Checkers

Geoff Cole

Mary Shafer

Scott A. Siege

Simson L. Garfinkel

Disclaimers in software

PGN

Junior Exec's Reverse Alchemy

Martin Howard

Yet another SSN misuse

Brian Clapper

EFF Summary of Public Interest NII Summit 29 Mar 1994

Stanton McCandlish

Info on RISKS (comp.risks)

Mud Slide Cuts East Coast Phones

"Peter G. Neumann" < neumann@csl.sri.com>

Thu, 31 Mar 94 15:05:32 PST

Telephone service to thousands of MCI Communications Corp. East-Coast customers was disrupted early in the morning of 30 Mar 1994 when a mud slide severed a fiber-optic cable. Calls into and out of the Washington D.C., Maryland, and Richmond VA areas were affected. Custromers in Miami, Atlanta, and St. Petersburg also reported disruptions. [Source: San Francisco Chronicle, 31 Mar 1994]

Briton Survives "Monster" Attack due to computer glitch

"Will Deatrick" <Will_Deatrick@smtp.esl.com> 31 Mar 1994 12:20:48 -0800

The 30 March 1994 issue of the San Diego Union contained a Reuters story from Land's End, England. It reads in part:

A mechanical sea monster designed to terrify tourists attacked and injured a set designer working on it ... the hydraulic tentacled beast went out of control because of a temporary fault in its computer program and held designer George Thain in its 3-foot toothed jaws for nearly a minute."

The man was badly bruised, but otherwise unharmed. The story does not state what corrective action is planned, but the town chairman ``assured visitors they would have nothing to fear from the monster, which will be kept 3 feet away from spectators."

Will will_deatrick@smtp.esl.com

[Also heard on NPR by gat@aig.jpl.nasa.gov (Erann Gat). PGN]

Risk Evasion Measures Create New Risks

"Stephen A. Stough" <sastough@rahul.net> Wed, 30 Mar 1994 18:25:42 -0800 (PST)

Final report blames Lucas design, Lockheed's procedures for HTTB crash

Federal safety officials yesterday blamed an inadequate actuator design by Lucas Aerospace and Lockheed's failure to take account of its shortcomings for the crash last year of Lockheed's one-of-a-kind High Technology Test Bed plane.

In its final report on the Feb. 3, 1993, crash at Dobbins AFB, Ga., the National Transportation Safety Board said the plane lost all rudder control during a high-speed taxi test with a simulated No. 1 engine failure when an experimental fly-by-wire control system for the rudder disengaged.

"The disengagement was a result of the inadequate design of the rudder's integrated actuator package by its manufacturer," NTSB said.

A design feature in the actuator removes hydraulic pressure if the rudder position commanded by the pilot exceeds the actual rudder actuator position for a specified time, and the rudder position trails, according to the report.

Lucas Aerospace designed the package, a self-contained unit configured to be a drop-in replacement for the existing Hercules/HTTB dual tandem rudder actuator.

The HTTB had recently been modified to evaluate power-by-wire flight control systems developed by Lockheed, along with some 50 suppliers. Lucas' package was demonstrated on two flights in March 1992, which Lockheed, claiming success, noted was the first time the concept had been tested on a manned flight.

Still, NTSB said that on at least one occasion the actuator had previously disengaged in flight, but "the company did not conduct a system safety review of the rudder bypass feature and its consequences to all flight regimes, nor of the (ground minimum control speed) test."

The fact that neither pilot was trained as a flight test engineer contributed to the accident, the report said.

"I do want to emphasize that the seven crew members were extremely qualified for the jobs they were doing," a Lockheed spokesman said in a prepared statement. "We still feel a great sense of loss for these colleagues and we praise their contributions to aviation. Beyond that, we prefer not to comment on the NTSB report, the investigation, or the accident."

The highly modified L-100-20 Hercules transport was not programmed to become airborne, NTSB Chairman Carl Vogt said shortly after the accident (DAILY, Feb. 5, 1993, page 200). But an NTSB spokesman told The DAILY yesterday that "it is the analysis of the board that (the pilot) attempted to get the plane airborne at that moment," although to this day nobody knows why the takeoff was attempted.

The report noted that the flight test plan specified that engine power be retarded if the rudder became ineffective. The aircraft was at full power but had not reached takeoff speed when it briefly became airborne, clipped a Navy clinic and crashed about 200 yards north of the runway, killing all seven aboard.

Lockheed said it was reviewing the NTSB's data, adding that "action will be taken as appropriate."

Rental cars and financial derivatives

Phil Agre <pagre@weber.ucsd.edu> Thu, 31 Mar 1994 15:34:26 -0800

The 3/30/94 New York Times includes two articles that illustrate the vexatious trade-offs inherent in emerging computer-based systems.

Matthew L. Wald, Two technologies join to assist lost drivers, New York Times, 30 March 1994, page A13.

This article is about a computer system that Nynex is developing, and that Avis will be testing, in which rental cars are kept in close contact with the rental agency through wireless communication. The technology is sold as a way of protecting drivers such as the tourists who were attacked in Florida; the cars will be equipped with "panic buttons" and the like. The article also

says that drivers will be able to call in for directions on wireless phones, with the phone operators having access to digitally encoded GPS information plotted against detailed maps, enough to be able to say "take the next left" remotely.

So far so good. But, at least the way the article describes it, the system will also allow the company to track all drivers for all purposes, regardless of whether they are in danger or need directions. A natural suspicion is that this generalized tracking capability is a major part of Avis's actual motives for promoting the systems. Motives aside, the privacy concerns may be serious in any case. How might these concerns be weighed against the advantages? How might the system be designed to obtain the advantages without the disadvantages? The article contains no hint that such questions are being asked, and this is unfortunate.

Barnaby J. Feder, Sophisticated software set for exotic financial trades, New York Times, 30 March 1993, pages C1, C5.

This article concerns "a marriage made in techno-geek heaven" between computer people and high finance, specifically software for analyzing and administering complex financial transactions based on so-called "derivatives" (see Risks 15.66). One virtue of these systems is that they reduce the possibilities for error, which are pretty serious when these kinds of transactions are done by hand. At the same time, such systems allow derivatives to be traded in much larger volumes, and in much more complex ways.

Much popular imagery associates derivatives with speculation, for example high-stakes gambling in commodity futures, but the real issue is almost the opposite. The usual purpose of these transactions is to engineer little islands of stability and predictability within the swirling chaos of global financial markets. Indeed the metaphor of "engineering" is frequently used -- the software discussed in the article is referred to as "financial CAD (computer-aided design)". The potential trouble comes when massive financial edifices are engineered badly. When a steel-and-concrete building falls down, the earth is there to catch it and a limited number of people get killed. But that's not how financial engineering works -- one collapsing structure has the capacity to take others down with it (again, see Risks 15.66). Obviously it's in their interest to be careful, but let's hope they know what they're doing.

Phil Agre, UCSD

White collar crime in Australia

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 30 Mar 94 08:20:52 EST

>From the Reuter newswire via Executive News Service on CompuServe (GO ENS):

CANBERRA, March 24 (Reuter) - White-collar crime is the most costly crime in Australia, totalling as much as Australian \$13.7 billion (\$9.8 million) a year, according to a report on Australia's law enforcement agencies.

Key points:

- o Committee included "representatives from the Australian Federal Police, the National Crime Authority, the Attorney-General's Department, the Finance Ministry and the Prime Minister's office."
- o Most white-collar crime is fraud.
- o Fraud "imposes the greatest economic cost on the Australian community of all forms of major and organised crime."
- o Annual cost of fraud A\$6.9-A\$13.7 billion (U\$4.9-\$9.8 billion) (about 2/3 of cost of all crime in Australia, estimated at A\$11-20 billion)

Michel E. Kabay, Director of Education, National Computer Security Assn

Hotline reassignment

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 30 Mar 94 08:20:47 EST

>From the Associated Press newswire via Executive News Service on CompuServe (GO ENS):

Telephone Sex

ST. JOSEPH, Mich. (AP, 25 March 1994) -- People calling a hot line for victims of domestic violence got a phone sex line instead when authorities didn't notice that the agency operating the hot line had closed.

Police habitually distribute cards with numbers of support services to victims. Seems that the hot line was reassigned to a number advertising various aural sex <g> services. No one bothered to check the accuracy of the card for two years.

[Consequence of poor quality assurance.]

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Electronic purse

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 30 Mar 94 08:20:56 EST

>From the Associated Press newswire via Executive News Service on CompuServe (GO ENS): [presumably 30 Mar 1994]

MARY BETH SHERIDAN, AP Business Writer, reports on new developments in electronic money.

NEW YORK (AP) -- Visa International is developing a do-it-all credit card that could pay for highway tolls, telephone calls or chocolate bars from

vending machines.

The company said Tuesday it is joining with an international group of nine other financial companies to develop the product, called the Electronic Purse."

Key points:

- o Consortium working on standards for interoperability.
- o Plastic smartcard with embedded processor.
- o Transfer money from their accounts to the smartcard. perhaps at automated teller machines.
- o Trials planned for late 1995.
- o Must equip phones, vending machines, stores with I/O devices.
- o Current costs \$3-\$8/card; expect drop to \$1 in high volume.

Michel E. Kabay, Director of Education, National Computer Security Assn

Dials!

<Bob_Frankston@frankston.com> Thu, 31 Mar 1994 09:47 -0400

My son (11) confronted a dial phone this past weekend and couldn't figure out how to use it. He tried pressing the "buttons" but nothing happened. We finally had to show him the concept of turning the dial. It took a little practice to get it smooth.

I guess we've reached a milestone. What if he were confronted by the "anti-drug" pay phones with dials and had to dial 911? He'd be stuck.

In designing UI's we make assumptions about cultural norms or icons. Most people see the phone dial as a very obvious interface. It isn't, it's just something most of us learned at an early enough age to assume it is a part of the natural world.

re: Spelling Checkers

Geoff Cole <ln1gec@entoil.co.uk> Wed, 30 Mar 94 10:15:05 BST

It is the bane of my life that spell-checkers offer the following suggestions for my name:
goof, gaffe and guff

Geoff Cole geoff@entoil.co.uk

Risks of spelling checkers (Girard, RISKS-15.71)

Mary Shafer <shafer@ferhino.dfrf.nasa.gov> Tue, 29 Mar 94 18:36:16 PST

The DECMate II spell checker offered NAUSEA for NASA. Singularly appropriate some days.

Mary Shafer, SR-71 Chief Engineer, NASA Dryden Flight Research Center, Edwards, CA shafer@ferhino.dfrf.nasa.gov

Risk of Spelling Checkers

Scott A. Siege <sie6@midway.uchicago.edu> Wed, 30 Mar 94 13:12:45 CST

I have read with interest the RISKs associated with spelling checkers and especially one in which a UNIX machine failed to recognize the word UNIX. A similar thing happened with a spelling checker for the Apple Macintosh which refused to recognize "Laserwriter" (Apple's printer) and instead suggested "Laserjet" (HPs printer).

-Scott s-siege@uchicago.edu

Next

Simson L. Garfinkel <simsong@next.cambridge.ma.us> Wed, 30 Mar 94 19:17:59 EST

NeXT is in the NeXT spell checker, but NeXTSTEP is not.

Disclaimers in software

"Peter G. Neumann" <neumann@csl.sri.com> Wed, 30 Mar 94 16:29:46 PST

We have had various past discussions on creative disclaimers. Someone very well known to me received the following, but I have anonymized everything to protect whomever.

You have our permission to use $[\dots]$ as an NTP server. Please do not configure more than two of your systems to communicate with $[\dots]$.

Please understand that [...] makes absolutely no guarantees about the reliability, availability, accuracy, or security of this service.

Also, please note that this service is likely to disappear fairly soon,

as it is based on a satellite that is about to fall out of the sky.

Junior Exec's Reverse Alchemy

MARTIN <MARTIN@411.uptown.com> 31 Mar 1994 16:35:09 +0800

Next time you get called into the bosses office, spare a thought for Juan Pablo Davila, who WON'T be winning "Employee of the Month" at Codelco.

An extract from an article in THE ECONOMIST (p.66.Feb 12, 1994):

SANTIAGO: Juan Pablo Davila claims that last September he made a mistake. He punched several 'sell' figures into his computer as 'buy', and vice-versa. Mr Davila was a fairly junior executive at Codelco, Chile's mammoth state-owned copper company. But he handled all Codelco's minerals futures contracts. By the time he noticed his slip he had already lost \$40m. So he kept on dealing; when his credit lines finally ran out in January, his losses had reached \$207m.

Mr Davila's mistakes pose troubling questions for Codelco. Why did nobody notice the losses? Did his superiors fraudulently extend Mr Davila's credit lines? Can any money be recovered? On February 5th Codelco's president resigned, admitting that the losses exposed a failure of internal controls...

MARTIN HOWARD, HONG KONG 31/3/93 MARTIN@411.uptown.com Tel: (852) 527 2123 Unit E, 9 Floor, China Overseas Building 139 Hennessy Road, Wanchai, Hong Kong

Yet another SSN misuse

Brian Clapper <bmc@tbsi.com> Thu, 31 Mar 1994 13:48:19 -0500 (EST)

A colleague informs me that, in conjunction with graduate courses he's taking at a local university, he was assigned an account on one of the University's computer systems. He was appalled to find out that his assigned computer ID was his social security number. When he asked whether he could change the computer account ID, he was told, "No. That's your account number." The system in question is on the Internet and apparently has a Usenet newsgroup feed, as well.

I won't bother to list the risks.

Brian Clapper Telebase Systems Inc., Wayne, PA

★ EFF Summary of Public Interest NII Summit 29 Mar 1994 [To many groups]

Stanton McCandlish <mech@eff.org>

Thu, 31 Mar 1994 17:57:54 -0500 (EST)

EFF SUMMARY

PUBLIC INTEREST SUMMIT: SHAPING THE NATIONAL INFORMATION INFRASTRUCTURE

Hyatt Regency Hotel in Washington, DC, MARCH 29, 1994

OPENING REMARKS

Welcoming remarks were delivered by Andrew Blau from the Benton Foundation, who expressed gratitude to the program sponsors and planning committee. Secretary of Commerce Ron Brown delivered pre-taped opening remarks on video, because he was in Russia at the time of the conference. Secretary Brown, who chairs the Information Infrastructure Task Force (IITF), restated the Administration's commitment to universal service, emphasizing that no one should be left standing on the side of the road.

PUBLIC INTEREST SUMMIT PANELS

DELIVERING THE GOODS: MEETING PUBLIC NEEDS?

Moderator: V. Lane Rawlins, President, Memphis State University
C. Everett Koop, Senior Scholar, Koop Institute
David Lytel, White House Office of Science and Technology
Jean Armour Polly, NY State Research and Education Network
Anthony Riddle, Chair, Alliance for Community Media
Connie Stout, Director, Texas Education Network
Patricia Waak, National Audubon Society

This panel discussed the ways in which the National Information Infrastructure (NII) can improve education, health care, and the environment by enhancing communication and decisionmaking within communities, as well as within state, national, and international boundaries. There was strong consensus on the panel and from the floor that teaching people to use the tools is as important as building the tools. Choosing the right regulatory model is a difficult issue, but David Lytel said that the Clinton Administration is committed to making sure that citizens can be information producers, as well as information consumers. He stated that the challenge is to make sure that the NII becomes more than just a large pipe for television reruns and movies, home shopping, electronic games, and gambling. The architecture of the NII must guarantee that needs outside the commercial marketplace, including cultural and other public benefits, are met.

A LINK INTO EVERY HOME: HOW, WHAT, AND WHEN?

Moderator: Allen Hammond, Director, Communications Media Center, NY Law School Ron Binz, Director, Colorado Office of Consumer Counsel Mark Cooper, Director of Research, Consumer Federation of America Deborah Kaplan, Vice President, World Institute on Disability Robert Larson, President/General Manager, WTVS-Detroit

Michael Nelson, White House Office of Science and Technology Andrew J. Schwartzman, Executive Director, Media Access Project

The panel explored the challenges in applying the concept of universal service to the NII to ensure access for everyone. The panelists discussed universal service funding mechanisms, the role of government in supporting a diversity of voices, and the need for public interest advocacy before the Federal Communications Commission. Mike Nelson said that the Administration's model for the NII is the Internet, and its goals for universal service are to provide subsidies to enable open access for as many people as possible, to adopt pro-competitive policies, to require nondiscriminatory prices, to prohibit network providers from controlling information, and to enhance interoperability and interconnection requirements.

Addressing the difference between the common carriage regime for telephone companies and the market/consumer model for the cable industry, Andrew Schwartzman argued for the common carriage model instead of the cable model, because the cable model is passive and connotes people receiving only limited services such as video-on-demand and home shopping. Common carriage would help NII users to be speakers as well as listeners, and producers as well as consumers. Ron Binz offered the phrase "Information Superhypeway" and cautioned that a fully competitive telecommunications industry is not right around the corner. The key decision, according to Binz, is whether to rely on taxing voice communications service to fund the NII. Binz also characterized as "industry propaganda" the view that subsidies should be provided to enable access for as many people as possible. Mark Cooper challenged the widely cited statistic that 93% of the population enjoys telephone service. Instead, he stated that the 7% "unsolution" is really closer to 30%, which includes individuals with disabilities and low incomes. He argued that those who cannot afford access to the NII will be assured access if everyone who can afford to use the NII is required to pay for it.

Deborah Kaplan took the discussion beyond the issue of funding to the issue of access. She argued that the 7% of the population that is underserved is a product of the market model. There is no one-size-fits-all solution, and policy input from low-income people is essential. She raised the concern that access to the NII for disabled individuals may be uniquely difficult, especially if the NII architecture is modeled on voice-based telephone service. Schwartzman emphasized the First Amendment dimension of universal service, including artistic speech, and the need to protect against any form of censorship. Bob Larson explained how public broadcasting's role in promoting local service responsibilities and public service duties is a model for what the NII can do to marshall local resources. The NII could augment public broadcasting's efforts aimed at reducing violence and improving the well-being of young people.

SPEECH BY VICE PRESIDENT AL GORE

The Vice President was introduced by Peter Goldmark, President of The Rockefeller Foundation, who emphasized the historical role of the NII in charting the future of democracy. Vice President Gore stated the

Administration's commitment to wiring every classroom, clinic, and library in the United States to the NII within the next five years. Every person will benefit from the NII. However, while we already have the technology, we do not yet have the infrastructure. The National Telecommunication and Information Administration in the Department of Commerce recently announced the availability of funding for some of the aspects of the NII and already have received 3,500 inquiries.

Reforming telecommunications law is essential. Universal service means lower prices for everyone. Open access means receiving and sending information across the NII. The future will look like the Internet if we make sure the NII is open and accessible like the personal computer.

Networked communities are consistent with our democratic form of government and distinguish it from communism and fascism. We need to increase access to government information to enhance community decisionmaking. We are increasing the availability of government information. SeniorNet is providing services to senior citizens. The Environmental Protection Agency's toxics release inventory is empowering citizens to ameliorate environmental hazards in their communities. HUD has begun to put information about fair housing and fair lending on the net. We can empower our representative democracy. People closest to the problems are the smartest about the solutions.

BUILDING COMMUNITIES AND THE ECONOMY

Moderator: Linda Tarr-Whelan, President and Exec. Dir., Center for Policy Alternatives

Morton Bahr, President, Communications Workers of America Cushing Dolbeare, President, Low-Income Housing Coalition Thomas Kalil, National Economic Council for Science and Technology Anthony Pharr, Counsel, Office of Communication, United Church of Christ Diana Roose, Research Director, National Association of Working Women Randy Ross, Vice President, American Indian Telecommunications

After brief introductory statements, the panelists discussed what the NII means for generating jobs and economic benefits. The goal is to use the NII to create better, high wage jobs. Development of information policy must make sure that the NII is a tool for community planning. Telecommuting will have an impact on the national economy by enabling people to live and work anywhere, including in other countries. We should use the technology that exists now in order to do the kind of planning needed to make sure the new technologies produce advances in our national economy.

MAKING DEMOCRACY WORK

Moderator: Sonia Jarvis, Exec. Dir., National Coalition for Black Voter

Participation

Brian Banks, Policy Research Action Group

Jim Butler, Director, AARP/VOTE, American Association of Retired Persons

Mitchell Kapor, Chair, Electronic Frontier Foundation Sally Katzen, Chair, Information Policy Committee, IITF Ralph Nader, Center for the Study of Responsive Law Nadine Strossen, ACLU

This panel addressed whether the NII can support increased civic participation, free speech and assembly, and privacy. Brian Banks stressed the NII's ability to bring about a reconfiguration of hierarchies; enhanced citizen participation in the decision making process would be the most fundamental change. Jim Butler revisited the NII's potential for community development, educational opportunity, and access to government databases. Mitchell Kapor focused on the potential for achieving the Jeffersonian principles of individual liberty and decentralization. The Internet has enormous democratic potential, but it is not easy to use. The emphasis should be on the Internet and interactivity, not on the Information Superhighway and Hollywood reruns. Everyone should become hands-on, start learning and interacting, and ask for help when needed. The networks should be easy to use, but we cannot wait for a national handout.

Sally Katzen stressed the goal of economic sustainable development. The government should not be solely responsible for the nation's information systems. The toxics release inventory is a model that has worked well. Ralph Nader, who still uses a manual Underwood typewriter, questioned what all this new technology will do about such problems as violence in the schools. Will it just put more people into the Office of Management and Budget and lead to mega-billion dollar overselling of unused software? While there needs to be a window on government databases, there is not reason for them to be overprivatized or overmonopolized. Educational efforts, like liberal arts-type courses, could motivate people to participate. Nadine Strossen argued that the common carriage model is important to ensure universal access--but security and privacy are equally important. We have to make certain that there are no censorial controls over content. All of us must lobby for privacy protection -- and we must fight the clipper chip.

Stanton McCandlish * mech@eff.org * Electronic Frontier Found. OnlineActivist "In a Time/CNN poll of 1,000 Americans conducted last week by Yankelovich Partners, two-thirds said it was more important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it."

- Philip Elmer-Dewitt, "Who Should Keep the Keys", TIME, Mar. 14 1994



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 73

Friday 1 April 1994

Contents

A320 software goes on "3rd Party" maintenance

Pete Mellor

Re: Risks of spelling checkers

Joseph T Chew

Andrea Chen

Eric Sosman

Re: Mud Slide Cuts East Coast Phones

David Lesher

Aural Sex and Rudder Actuators

A. Padgett Peterson

More jail-door openings

Tom Markson

PGN

find/xargs strangeness

Peter J. Scott

Chris Dodd

P. R. China Computer Security Rules

John Ho

Info on RISKS (comp.risks)

★ A320 software goes on "3rd Party" maintenance

Pete Mellor <pm@csr.city.ac.uk> Fri, 1 Apr 94 23:52:42 BST

While I was in Copenhagen earlier today, a Danish friend, who knows of my interest in the A320, drew to my attention an item in today's issue of the news magazine "Goddaj" (if I recall the spelling correctly - it means "Good Morning"). A translation of the article follows (courtesy of my Danish friend):-

-----Translation of Article in "Goddaj", 1st April 1994 -----

Danish Firm Scores Notable "First"

Thor Avionics, one of Denmark's most advanced high-tech firms, has secured a contract which makes it the first software house in the world to provide "third party" maintenance on a major safety-critical software system.

In order to reduce the maintenance costs on its fleet of Airbus A320 aircraft (the first type of civil airliner in the world to have a computer-controlled "fly-by-wire" system), Air France has placed Thor under contract to provide all future maintenance on the software of this highly-automated aircraft.

Wolf Larssen, director of Thor, said "This is the first contract of its type, and it won't be the last. Users of commercial software long ago discovered that there are great savings to be made by getting a "third party" firm to maintain their software. I am only surprised that it has taken users of safety-critical systems so long to discover the advantages. I expect other A320 operators to be placing similar contracts before too long."

A "third-party" in this context means a firm which is independent of both the user and the supplier. Such firms, being "lean and mean" are usually capable of providing a much better and more cost-effective service than the original supplier, since they have fewer overheads and are less stifled by bureaucracy. In the commercial world, such contracts have usually gone to small, dynamic, organisations, and it seems that the world of safety-critical software will follow suite.

"We had to beat some stiff opposition from Sextant Avionique, Matra, Logica, and similar large firms." said Mr. Larssen. "The fact that the software on the A320 will need to be maintained indefinitely means guaranteed jobs for highly qualified Danish workers for a long time to come."

M. Theophile Gautier, spokesman for Air France, said "We have the utmost confidence in Thor to deliver the goods, both in terms of reduced cost, improved system performance, and increased safety."

The automated systems on the A320, particularly the flight control and flight management systems, have sometimes been called into question following the various accidents involving this type of aircraft, although the accidents have generally been ascribed to pilot error. Even so, there is an obvious question mark over the ability of a third-party firm to maintain the level of safety.

When asked about this, Mr. Larssen said "Our software maintenance and validation process is second to none. Although Airbus Industrie have refused to release the source code, so that we will have to strip out the binary and work from that, we anticipate no problems. Most of the modifications we will be making are fairly slight, so that regression testing can easily be done on a software flight simulator running on an Apple MacKintosh."

A spokesman for the JAA (Joint Aviation Authority, which is responsible for certifying that any new or modified design of aircraft is airworthy) said "The basic design has already been certified. All that Thor will be doing are minor post-certification modifications. Thor themselves have been certified as conforming to the ISO-9000 quality standard and to SEI level 2,

so it should not be difficult for them to meet the requirements for our own certification, which is based upon an industry standard referred to as RTCA-DO/178B."

In response to questions about what the maintenance would actually involve, Mr. Larssen said "Occasionally, Airworthiness Directives are issued by the JAA which require changes to be made to the design of an aircraft in order to correct a fault. Where this change involved modifying the software, Thor will be responsible for doing this. The beauty of software is that the modified version can be installed on all existing aircraft in seconds, simply by inserting a new eprom. In addition to this corrective maintenance, we will also be offering Air France enhancements to improve the performance of the A320. The practice of "chipping", or modifying the firmware in the engine management system of an automobile such as a BMW in order to make it go faster, is well established. I don't expect that we could make your A320 perform like an F-111, but we could certainly extend the "safe flight envelope" beyond the rather conservative limits originally set by the manufacturer."

 Article	Ends	

I leave it to readers to draw their own conclusions!

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq London EC1V 0HB +44 (71) 477-8422, p.mellor@csr.city.ac.uk

[This is quite a Thor-ny piece. Incidentally, I note that "goddaj" is really "good day" (albeit used in the morning, as in the case of Guten Tag), and April 1 is certainly a "goddaj". Unfortunately, occasional adjacent-key typing errors might easily replace the "j" with an "m", which might be an appropriate reaction. PGN]

"I have a spelling checker, it came with my PC..."

Joseph T Chew <jtchew@Csa3.LBL.Gov> Fri, 1 Apr 94 09:45:46 PST

> NAUSEA for NASA. Singularly appropriate some days.

Microsoft Word's persistence in attempting to substitute Colada for Collider certainly made me feel the need for a drink when writing about the SSC...

--JOe

Re: Risks of spelling checkers

<tada@MIT.EDU> Fri, 1 Apr 94 11:17:19 -0500

The main risk is in relying too heavily on spell-checkers. As people produce more of their own documents, they no longer have someone who does most of the

proof-reading, and rely on a program instead.

Automation of other parts of document production has caused a change in the type of errors that can get through. Up until a few years ago, most errors in trade books were switched letters ("b" for "d") probably caused by manual typesetting. Now one finds many more mistakes of a wrong word, no doubt from a spell-checker substitution. Perhaps we can ask, who checks the spell-checkers?

-michael j zehr

★ Re: Risks of spelling checkers

Andrea Chen <dbennett@crl.com>
1 Apr 1994 01:00:42 -0800

By definition, a spell checker is a product which eliminates a large set of errors in a text. It does not eliminate them all. I would suggest that you do not go onto "auto pilot" when using the spell checker. Instead use the same level of awareness that you do when your write. In fact it makes sense to examine the text around every place the spell checker stops. There are a lot of errors which can only be eliminated by human attention. As far as I can see your general problem would not be eliminated by getting rid of profanity. Suppose you had a "Ms. Gorse" in your document. A spell checker might offer "Goose". Your client (or boss) might be equally offended.

Risk of Spelling Checkers

Eric Sosman x4425 <eric@tardis.hq.ileaf.com> Fri, 1 Apr 94 13:23:55 EST

A company which sometimes competes with my employer sells a software package which includes a spelling checker. It flags

Re: Mud Slide Cuts East Coast Phones (Re: RISKS-15.72)

David Lesher <wb8foz@netcom.com> Fri, 1 Apr 1994 10:28:32 -0500 (EST)

Note this took out a reported 200+ DS3 circuits. That's ~~100,000+ voice-grade circuits (if all were such).

Netcom's DC POP was one of the DS1's. They had leased the circuit from WilTel, but WilTel in turn had subcontracted the facilities from MCI. Further, while MCI had the cable back up by 11pm, somehow WilTel did not communicate this to Netcom. Thus the POP was not restored until the next morning. (Irony here - WilTel got started pulling fiber through abandoned oil pipelines. Schedule 300 pipe provides much better than average protection against backhoe fade.)

Classic RISKs:

- 1) Too many eggs in one basket. While MCI surely has reserve capacity, it does not seem to have 200 DS3's worth. No self-healing ring, it seems.
- 2) Lost-in-translation syndrome Once more than two organizations are involved, the chances of getting any intact message from one end to the other goes down as an exponential function of the number of hops.

ps: Ispell wants to turn "WilTel" into "Wilted".......

✓ Aural Sex and Rudder Actuators (RISKS-15.72)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Fri, 1 Apr 94 08:05:49 -0500

It is interesting that both of these incidents have a common thread no feedback loops.

Way back in the '70s when I was part of the team that designed the full authority digital flight control system for the AFTI F-16, we had a similar problem: the system was so complex and so many people were involved that it was easy to miss the change that Jon made today would affect Harold's system and this was during the design stage. In production, component substitution could have the same effect, some so subtle that it would not be noticed until a pilot found himself in an interesting situation.

One of my tasks was to develop the simulation software used in a 40 foot Evans & Sutherland dome & as such with each revision of the flight control software, the appropriate changes had to be fed into the dome system.

In order to maintain continuity we developed a "configuration control model" that simply scanned the source code for all uses of a variable or subroutine and provided a map of the points of contact for each variable. When a change occurred, it was a simple matter to report the change to each affected engineer/programmer. It was also an excellent tool for reporting when someone had accidentally used the wrong variable in an equation since it would suddenly show use in a routine it had not been used in before.

This tool also made it possible to notify those responsible for affected modules when a component change was made since the tree for the variables used with the component was readily available.

The process was really simple but deductive rather than inductive: changes were detected not by people submitting a change notice but by a comparison of "current" versus "last", active configuration management rather than passive. Several times changes were found before the paperwork arrived.

The simple fact is that any large system, from a telephone number list to aircraft fight controls is subject to Chaos math: small omissions over time will increase in effect. Murphy says that unknown effects will be destructive. Multiple omissions multiply effects.

The most effective answer I have found is active feedback loops, something computers are very good at. Today one way I protect sites from intruder attacks is by requiring modem registration and briefing of owners. I also conduct random sweeps of the telephone lines looking for unregistered modems. Without the second, the first would rapidly become obsolete. This has two advantages:

- 1) I find omissions quickly.
- 2) People are less likely to make omissions knowing that they will be noticed.

Over the last few years I have seem many instances in RISKS of problems with aircraft flight controls making the wrong decision or telling the pilot the wrong thing and each time have wondered if active design or configuration management feedback loops could have prevented them.

Padgett

✓ More jail-door openings

Tom Markson <tom@twilight.com> Fri, 1 Apr 1994 12:54:43 -0800 (PST)

I saw on San Francisco's channel 4 last night that a jail in Marin which houses such people as Polly Klaus' killer has been having problems with their cell doors. Apparently, without reason, they would just open. The prison said their was no danger in escape. They blamed the problem on "software errors".

How about that?

--tom



RISKS Forum <risks@csl.sri.com> Fri, 1 Apr 94 14:27:06 PST

The RISKS archives include the following items from the ACM SIGSOFT Software Engineering Notes (S vol i no j). Recent items also appear in the on-line RISKS. PGN

..... Prison problems

Seven Santa Fe inmates escaped; prison control computer blamed (S 12 4) Oregon prisoner escaped; frequent-false-alarm alarm ignored (S 12 4) New Dutch computer system frees criminals, arrests innocent; old system eliminated, and no backup possible! (S 12 4)

New El Dorado jail cell doors won't lock -- computer controlled (S 13 4) San Joaquin CA jail doors unlocked by spurious signal; earlier, inmates cracked Pelican Bay State Prison pneumatic door system (S 18 2:4)



find/xargs strangeness

```
Peter J. Scott <pjs@euclid.jpl.nasa.gov>
1 Apr 1994 21:10:38 GMT
Man, just when I thought I understood this stuff. I have condensed
this down to the following:
euclid% euclid% mkdir something_scwewy
euclid% cd !$
euclid% foreach i (a b c d)
? echo $i > $i
? end
euclid% find . -type f -print | xargs -n1 more
./b
./c
./d
--More--(Next file: ./a)
                           # Hit <SPACE>
./a
euclid%
Now, to my way of thinking, it should be executing the commands "more ./a;
more ./b; more ./c; more ./d". Certainly I have had and come to expect this
sort of behavior from xargs in the past. It seems to be a problem with
"more", because I get decent behavior with, say, "echo" and "cat":
euclid% find . -type f -print | xargs -n1 cat
b
d
Yet:
euclid% find . -type f -print | xargs -t -n1 more
more ./a
./b
./c
./d
BTW, if there are more than a screenful of files, I get prompted by
more to scroll through the list of them before it actually runs
more on the first file. I don't get this at all. This is on SunOS 4.1.3.
Peter Scott, NASA/JPL/Caltech (pjs@euclid.jpl.nasa.gov)
```

Re: Peter J. Scott: find/xargs strangeness]

Chris Dodd <dodd@csl.sri.com> Fri, 1 Apr 94 15:05:31 -0800 This is an example of a strange interaction of two bugs, one in 'more' and one in 'xargs'. All bugs are RISKS to some extent, its not clear how severe or unusual they need to be to make it into RISKS...

There are two strange things occurring here.

- 1. When 'more' is invoked with its standard input connected to something OTHER than a terminal, it treats 'stdin' as the first file to display.
- 2. 'xargs' doesn't close the input to the child it invokes.

So what happens is, 'xargs' invokes 'more ./a', and 'more' reads everything it can from its standard input, which connects to the 'find'. When 'more' finishes, 'xargs' finds that its 'stdin' is empty and exits.

To exercise these bugs separately, try: echo a b c | more ./a echo a b c d | xargs -n1 cat -

Chris Dodd dodd@csl.sri.com

P. R. China Computer Security Rules (long)

<[a known contributor who wishes to remain anonymous]> Fri, 1 Apr 1994 12:22:17 (xxT)

connection to the Internet (CHINANET; sub CHINANET to LISTSERV@TAMVM1.TAMU.EDU).

The Chinese have named their new project to connect China to the Internet the "Golden Bridge" project. The following document purports to be the newly developed "PRC Regulations on Safeguarding Computer Information Systems." It seems quite appropriate for RISKS.

As you read this, keep in mind that 1) in China accused persons are guilty until proven innocent; 2) laws referred to in the document as ones applying in certain circumstances are often harsh, subject to change without notice, and so vaguely worded as to make easy the prosecutor's job, not of proving guilt (not necessary), but of arguing why the penalty should be maximized; 3) the "Public Security" laws referred to are the same laws that stipulate that the families of serious offenders will be billed for the single bullet used in judgement; 4) certain concepts (virus, special security products) are either poorly defined or all inclusive; 5) in China when there is doubt as to the legality of any particular act, illegality is assumed (this is important not only in court, but also in normal life, where people tend to be more conservative in part because of it.)

As we welcome this brave new domain into our net.universe, it will be interesting, and perhaps surprising at times, to see how another set of explorers on the electronic frontier are approaching the flow of information. Golden Bridge, indeed. As read, sending email without filing a customs declaration, or accepting a shareware registration for an anti- virus product could both be construed as being illegal. There's a lot of room for

Source: Beijing XINHUA Domestic Service in Chinese, February 23, 1994 From: john@jho.com (John Ho), Asia Online

Chapter I. General Provisions

Article 1. These regulations have been formulated to safeguard computer information systems, to promote the application and development of computers, and to ensure smooth progress in socialist modernization.

Article 2. The computer information systems referred to in these regulations are man-machine systems, composed of computers and their allied and peripheral equipment and facilities (including networks), that collect, process, store, transmit, and retrieve information according to prescribed goals and rules of application.

Article 3. In safeguarding computer information systems, measures shall be taken to secure computers, allied and peripheral equipment and facilities (including networks), the operating environment, and data, as well as to ensure the normal functioning of computers, so as to safeguard the safe operation of computer information systems .

Article 4. In safeguarding computer information systems, priority shall be given to the security of computer systems containing data on such important areas as state affairs, economic construction, national defense, and state-of-the-art science and technology.

Article 5. These regulations shall apply to safeguarding computer information systems within the PRC's borders.

Measures for safeguarding microcomputers that have not been hooked up shall be enacted separately.

Article 6. The Ministry of Public Security shall be in charge of safeguarding computer information systems.

The Ministry of State Security, the State Secrecy Bureau, and relevant State Council departments shall carry out work pertaining to safeguarding computer information systems within the lines of authority prescribed by the State Council.

Article 7. No organization or individual may use computer information systems to engage in activities that endanger national or collective interests, as well as the legitimate interests of citizens; they may not jeopardize computer information systems.

Chapter II. The Safeguards System

Article 8. Computer information systems shall be established and applied in

accordance with laws, administrative rules, and relevant state provisions.

Article 9. Computer information systems shall be protected on the basis of security grades. The Ministry of Public Security, in conjunction with relevant departments, shall establish security grades and formulate specific measures for protection based on such grades.

Article 10. Computer rooms shall conform to state norms and relevant state provisions.

No work may be carried out in the vicinity of computer rooms that jeopardizes computer information systems.

Article 11. Units using internationally networked computer information systems shall register their systems with the public security departments of people's governments at or above the provincial level.

Article 12. Individuals who ship, bring, or mail computer information media into or out of the country shall file truthful declarations with the customs authorities.

Article 13. Units that use computer information systems shall establish security management systems and assume responsibility for safeguarding their computer information systems.

Article 14. Units that use computer information systems shall report any incidents relating to their systems to the public security departments of local people's governments at or above the county level within 24 hours of the incidents.

Article 15. The Ministry of Public Security shall exercise centralized management over research into the control and prevention of computer viruses and other harmful data that jeopardizes public security.

Article 16, The state shall implement a licensing system for the sale of special safety products for computer information systems. The Ministry of Public Security shall enact specific measures in conjunction with relevant departments.

Chapter III. Supervision Over Security

Article 17. Public security organs shall perform the following functions to supervise efforts to safeguard computer information systems:

- (1) Supervising, inspecting, and guiding the work of safeguarding computer information systems;
- (2) Investigating and dealing with illegal and criminal cases involving the endangerment of computer information systems; and
- (3) Other supervisory functions with regard to safeguarding computer information systems.

Article 18. Upon detecting latent hazards in computer information systems, public security organs shall promptly advise the units that use such systems to institute safety measures.

Article 19. Under urgent circumstances, the Ministry of Public Security may issue special circulars on specific security aspects of computer information systems.

Chapter IV. Legal Responsibilities

Article 20. In the event of any of the following violations of the provisions in these regulations, public security organs shall issue warnings or shut down the computers for screening purposes:

- (1) Contravening the system for protecting computer information systems based on security grades and jeopardizing computer information systems;
- (2) Violating the registration system for internationally networked computer information systems;
- (3) Failing to report incidents related to computer information systems within the prescribed time frames;
- (4) Failing to take remedial action within the prescribed time after receiving notification from public security organs mandating security improvement measures;
- (5) Other actions endangering computer information systems.

Article 21. Public security organs, in conjunction with relevant units, shall deal with cases in which computer rooms do not conform to state norms or relevant state provisions, or in which work carried out in the vicinity of computer rooms endangers computer information systems.

Article 22. The customs authorities shall deal with failure to file truthful declarations on computer information media shipped, brought, or mailed into or out of the country, pursuant to the "PRC Customs Law" and the provisions outlined in these regulations and other laws and regulations.

Article 23. Public security organs shall issue warnings or impose fines of not more than 5,000 yuan and 15,000 yuan, respectively, on individuals or units if computer viruses or other data harmful to computer information systems are deliberately input into such systems, or if special safety products for computer information systems are sold without permission. They shall confiscate illegal proceeds and impose a fine that is 100 or 300 percent more than the sum of such proceeds.

Article 24. Actions that violate the provisions in these regulations and constitute infractions of public security shall be punished pursuant to relevant provisions in the "PRC Regulations on Security Administration and Punishment"; if the actions constitute a crime, criminal responsibilities shall be investigated.

Article 25. Any organization or individual who inflicts property losses on the

state, collectives, or other individuals in violation of the provisions in these regulations shall assume civil responsibility in accordance with the law.

Article 26. Interested parties who are dissatisfied with specific administrative actions carried out by public security organs pursuant to these regulations may apply for administrative reconsideration in accordance with the law or file administrative lawsuits.

Article 27. Government functionaries who abuse their power to demand and take bribes or commit other illegal or delinquent acts while enforcing these regulations shall be punishable on criminal grounds if their actions constitute crimes or given disciplinary actions if their actions do not constitute crimes.

Chapter V. Supplementary Provisions

Article 28. The meanings of terms used in these regulations are defined as follows:

Computer viruses mean a set of self-replicating computer commands or programming codes inserted during the course of programming or into computer programs that can impair computer functions, destroy data, or affect computer use.

Special safety products for computer information systems mean special hardware and software products for use in safeguarding computer information systems.

Article 29. Military-related computer information systems shall be safeguarded in accordance with relevant military laws and regulations.

Article 30. The Ministry of Public Security may formulate implementation measures in accordance with these regulations.

Article 31. These regulations shall take effect upon promulgation.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 74

Saturday 2 April 1994

Contents

Re: Spell checking

J. Taggart Gorman

Pete Mellor

Castor Fu

Les Earnest

Re: Language ability is not entirely learned

Paul Colley

Re: Spelling, punctuation, poor language technology **Bill Stewart**

Re: English spelling design

Christopher Upward

Info on RISKS (comp.risks)

★ Re: Spell checking (RISKS-15.71)

Jonathan Haruni < jharuni@london.micrognosis.com> 31 Mar 1994 13:57:32 GMT

The only risk I see in spelling checkers is that people may trust them too much, or even expect too much of them. This is a widepsread risk of every technology.

- 1) You suggest that "it is easy to go unconscious in front of the mouse and press 'replace' one too many times". Surely a program which replaces words of your document without any knowledge of their meaning or intention is not one with which you should go "unconscious", especially when applying it to a document which, as you suggested, could lose you your job.
- 2) Your use of "business" and "profane" are a bit misleading. What you really want is a checker which does not suggest words which are inappropriate to the purpose of your document (making money from customers). How is that possible? Whatever a document says, there are valid words which express the opposite ideas. You cannot omit from the dictionary all the words which might cause offence to anyone doing

"business". Even if you did, add or omit the word "not" in a suitable place in a business proposal, and you could lose a customer. Can a business document not contain profanities if it suits the purposes of the document?

3) Can you really blame the SPELLING checker for suggesting a common English word in place of a proper name? I have never seen a spell checker which did not allow you to augment the dictionary. The first thing a company should do is add all the names and addresses of every organization it deals with. Have you done that?

I suggest that you have bought a useful tool (spelling checker), failed to make the effort of tailoring it to your needs (adding your correspondents to the dictionary), and expected too much of it (to provide you with a document which fulfills your intentions, rather than merely one without spelling errors). Then you fed it a document with so many errors that you became complacent about its power (not paying conscious attention to its prompts for confirmation). In spite of all this, it corrected your spelling mistakes and you DID notice the "goddamn" suggestion when prompted, so you ended up with a better document.

Where are the risks?

Jonathan Haruni.

★ Re: RISKS of RISKS on spelling-checkers

J. Taggart Gorman <taggart@scopus.com> Fri, 1 Apr 94 17:09:51 PST

It seems that some RISKS contributors are engaged in an activity that should not be discussed on a computer-related list such as this: spellcasting. However, it is obvious that they are using their computers to help with their witchery, for they keep on mentioning using "spell-checkers". At least we know that modern technology is helpful to all, including spellcasters. On the side, I've never seen a "spell-checker" for sale in a computer store. Are they commonly available in occult stores? (Available on the Microsoft Occulta CD?)

:) (Not April's Fools, but with a light content for the day.)

Taggart Gorman taggart@scopus.com

★ Re: Risks of spelling checkers (Girard, RISKS-15.71)

Pete Mellor <pm@csr.city.ac.uk> Sat, 2 Apr 94 21:02:14 BST

- > with the suggestion that the word "Goldman" (as in a large company we all
- > know) should be replaced with "goddamn". The word processor involved was MS

-----From the Daily Mail, Friday April 1st 1994, p21-----

Don't you dare be sexist says the PC PC, by Suzanne O'Shea

The new computer program promised to help users write better English.

But buyers have ended up with more than they bargained for. As well as a guide to glitch-free grammar and scintillating syntax, they get a lesson in political correctness every time they switch on.

The use of words such as `wife', `policeman' and `housewife' meets with a sharp rebuke from the software, which flashes up a message that they are `gender-specific' then provides `gender-neutral' options such as `spouse', `police officer' and `homemaker'.

Anyone foolish enough to test the PC personal computer with words such as 'little woman' or 'girlie' is sternly informed that they are 'sexist expressions'. No alternative is offered here, only the ominous message: 'Avoid using this word.'

Computer writer Mark Smithson, 51, of Bedford, risked the wrath of the {pounds} 250 Microsoft Word 6 package when he typed in the word `freeman'. The computer promptly spat back `citizen'.

`I couldn't believe it,' he said yesterday. `Then I started going through lots of other sexist and "gender-specific" words and, sure enough, the same thing happened.

'It's like Big Brother. Manipulating what people write is a form of censorship. I am the last person to be deliberately sexist but this is downright frightening.'

In the politically correct world of Word 6 - produced by an American firm - users are advised to replace `mankind' with `humankind' or `humanity' - although `womankind' passes through without a hitch - and to replace `fireman' with `stoker'.

Its scope is limited when it sees words which it has not been told are sexist. While `little lady' may result in the reprimand `sexist expression, avoid using this phrase', followed by the explanation that `this term is considered by many to be inappropriate and belittling when used to refer to women', the word `floozie' is freely allowed.

No mention of the programme's political correctness was mentioned [sic: Perhaps Ms. O'Shea should use a style checker! - PM :-)] in publicity material when Word 6 was launched in Britain recently. Neither is the feature listed in the 830-page manual.

A Microsoft spokesman - sorry, spokeswoman, we mean spokesperson - defended the program yesterday.

'It does not force users to change what they write,' she said. 'It simply highlights words that might be regarded as sexist and suggests alternatives.

'Microsoft is trying to bring its programmes in line with real life and how people actually work. This type of thing is a sign of the times, as people do say chairperson instead of chairman nowadays.'

[Disclaimer: I don't *think* this is an April fool joke (if only because, if it were not true, Bill Gates would sue the Mail), but if it is, I didn't make it up! :-) Peter Mellor, Centre for Software Reliability, City Univ., Northampton Sq., London EC1V OHB +44 (71) 477-8422 p.mellor@csr.city.ac.uk

More spelling checker stories

Castor Fu <castor@drizzle.Stanford.EDU> Fri, 1 Apr 1994 18:01:42 -0800 (PST)

When cleaning up one day we found a portable spelling checker. To test the size of its vocabulary, we tried out some proper names. We were dismayed to find it suggesting "a**hole" [censored by PGN] as a correction for "Achille", my housemate's name. This was particularly unimpressive, as "Achilles", the more common spelling, was actually in its dictionary, but was not among any of the alternatives, which included a number of other unflattering possibilities.

-Castor Fu castor@drizzle.stanford.edu

✓ Risks of spelling checkers (RISKS 15.72)

Les Earnest <les@sail.stanford.edu>
2 Apr 1994 03:26:54 GMT

The earliest spelling checker was evidently one that was part of a pen-based computer system for cursive writing recognition that I developed at MIT Lincoln Lab in the 1959-61 time period. It was set up to recognize the 10,000 most common English words.

Sometime in 1961 a film crew from BBC came to the lab and asked to photograph the handwriting recognizer as part of a television program on advanced technology, to which I agreed. After setting up, they asked if the system could recognize the word "television." I agreed to give it a try but pointed out that it sometimes listed more than one word if it wasn't sure. After I wrote the word on the CRT with a light pen, the system paused only a second or two before responding:

TEDIOUS TELEVISION

The film crew loved it and zoomed in for a close-up! I've often wished that I had asked for a copy of their film.

Les Earnest (Les@cs.Stanford.edu) Phone: 415 941-3984 Computer Science Dept.; Stanford, CA 94305 Fax: 415 941-3934

★ Language ability is not entirely learned (Ranum, RISKS-15.69)

Paul Colley <colley@qucis.queensu.ca> Sat, 26 Mar 1994 23:41:54 GMT

>Spelling mistakes are a result of inattention to detail, ignorance, or apathy.

Which makes poor spelling sound like a deliberate decision. I assure you I am neither inattentive to detail nor apathetic about my poor spelling abilities. I like to think I'm not ignorant...

In my defense, I'll note that there is some strong evidence that language is based, at least in part, on genetics. Thus some portion of language skill is beyond the control of the individual.

Quoting from Jay Ingram's book, "Talk Talk", pp.133-141, there is...

"...a gene that makes it possible for most of us to be able to add an `s' to a word to make it plural, or choose `he' instead of `they' when it's appropriate, or add `ed' to a word when it happened in the past! Apparently if you inherit a faulty version of this gene you will never be able to do any of those automatically.

[...]

These people aren't aware that they have a problem making plurals or past tenses, [...]

[...]

This discovery [...] makes it much more difficult to argue that language is simply a byproduct of learning, [...]

The defect occurs in non-English speakers also. The gene seems to only affect language, and only the ability to make plurals and past tenses. If there's a gene for plurals, there are probably genes for other components of language.

Reference: Myrna Gopnik, linguist at McGill University, "Linguistic Properties of Genetic Language Impairment," address to the American Association for the Advancement of Science, February 10, 1992, Chicago.

- Paul Colley colley@qucis.queensu.ca +1 613 545 3807

Re: Spelling, punctuation, poor language technology

<wcs@anchor.ho.att.com> Sun, 27 Mar 94 03:46:51 EST

Aside from all the flames about whether spelling and punctuation

errors come from poor language design (:-) or poor user education or differences in values, there *are* some new technology-related problems. Many maga- zine articles, especially in the com- puter industry, are suffering from leftover hyphen- ations, which come from re-for- matting word-processed text and not checking whether -'s at the ends of lines are intentional dashes or are hyphens put in to accommodate line-breaks before including the - and space in the new text.

"Wired" is one of the worst offenders, probably because most of its authors use a variety of computer systems to write on.

Bill Stewart

[RISKS readers will notice that I try to REMOVE hyphenations whenever I spot them.

Other comments on this subject were received from brewer@cs.wmich.edu (Steven D. Brewer) and albaugh@agames.com (Mike Albaugh). PGN]

English spelling design

<c.upward@aston.ac.uk>
Tue, 29 Mar 1994 18:38:29 +0000

I just picked up the Don Norman/Mark Jackson/Alayne McGregor exchange on 'its', 'it's', and English spelling design generally.

Don is right about bad spelling design being the cause of endless problems of written English. But Halle & Chomsky were wrong about underlying deep consistency in English spelling. For one thing, their analysis ignored such fundamental inconsistencies as <ea/ee> in 'speak/speech'. For another thing, they ignored the whole historical dimension, which Don Norman rightly alludes to.

The truth is that for 1,000 years no one has been able to ensure consistency, deep or otherwise, in English spelling, ie since the Norman Conquest of England in 1066, English spelling, unlike that of most languages, has not been "designed with the user in mind", as Don Norman very sensibly puts it. Webster's contribution was a small step in the direction of greater consistency, which the British have still largely failed to follow. Various people have tried using extra symbols (Benjamin Franklin was one), but they have always run up against the problem of needing to teach all th millions (billions?) of potential readers what these new symbols stand for.

As for the apostrophe, the deep INconsistency of English rears its head there too. Mostly the possessive apostrophe precedes final <s> with singular nouns: 'the dog's kennel', but follows it in the plural: 'the dogs' kennels'. But sometimes we find the reverse: 'men's' is plural, but 'Achilles' is singular.

A different set of inconsistencies affects the possessive pronouns mentioned by Mark Jackson. As he rightly says, most don't use apostrophes, so that we write 'hers', 'ours', 'yours', 'theirs', and of course 'its', and not 'her's',

'our's' etc. But 'one's' is an exception: for some reason we DO write that with an apostrophe. However, the craziest inconsistency is 'whose', where we add an <e> at the end!

If Alayne McGregor implying that all languages are written as inconsistently as English, he is mistaken. English is unique - as are its problems of illiteracy. Both the USA and Britain have recently published major reports on its appalling extent.

We do need to get to grips with this question of spelling design. Let me now attach a recent paper put out by the Simplified Spelling Society on the subect.

Simplified Spelling Society World HQ c/o Bob Brown, 133 John Trundle Court, Barbican, London, EC2Y 8DJ, tel. 071-628 5876.
US HQ c/o Ken Ives, 401 E 32, Apt 1002, Chicago IL 60616.

CUT SPELLING

A Streamlined Writing System for English

a proposal for modernizing English spelling by removing redundant letters Enquiries to Chris Upward
Chairman of the Society's Cut Spelling Working Group
61 Valentine Road, Birmingham, B14 7AJ, England
Tel. 021-444 2837, Fax. 021-359 6153.

THE BACKGROUND

Why reform English spelling?

English spelling is notoriously hard to master. It is a centuries-old writing system whose contradictions and eccentricities were never designed for a fully literate society. We all suffer from its clumsiness and inconsistency: it takes far longer to learn than more regular systems; it limits people's ability to express themselves; it causes mispronunciation, especially by foreign learners; most people acquire at best an erratic command of it (even skilled writers are prone to uncertainty and error); and many millions are condemned to functional illiteracy. It is therefore small wonder there is such concern about standards of literacy in English-speaking countries today. Yet many of those countries have in recent decades seen the benefit of modernizing equally antiquated systems of currency and weights & measures. Similar modernization of English spelling is badly needed.

Is reform possible?

Spelling reform is an unfamiliar idea to the English-speaking world, but other languages show it is feasible and indeed a normal way of preserving a writing system from obsolescence. The letters of the alphabet were designed to stand for the sounds of speech, but pronunciation evolves in the course of time, and confusion sets in when letters and sounds cease to match: the way we speak words now no longer tells us how to write them, and the way they are written

no longer tells us how to speak them. That is the central problem of English spelling. In the past century many languages have modernized their spelling to improve this match between letters and sounds, and so aid literacy. To ensure continuity, only small changes are usually made, and while schoolchildren learn some new, improved spellings, most adults continue to write as before. It may therefore take a lifetime before everyone uses the new forms. Ideally, spelling reform needs to be an imperceptibly slow, but carefully planned and continuous process.

Problems of regularizing

Many schemes have been devised for respelling English as it is pronounced, but apart from some small improvements in America none has been adopted for general use. Several fully regularized systems have however been tried in the past 150 years in teaching beginners, with dramatic success in helping them acquire basic literacy skills, the best known recently being the i.t.a. (initial teaching alphabet). However, all these schemes have required learners to transfer to the traditional irregular spelling as soon as they can read and write fluently, and much of the advantage is then lost.

Ideal though total regularization may ultimately be, the effect such schemes have on written English is so drastic as to be a major deterrent to their adoption. The following sentence, in the Simplified Spelling Society's New Spelling (1948), perhaps the best thought-out and most influential of these fully regularized orthographies, demonstrates the effect:"Dhe langgwej wood be impruuvd bie dhe adopshon of nue speling for wurdz". Less radical proposals have therefore been made since then, so as to avoid such visual disruption, suggesting for instance that at first only the spelling of one sound, like the first vowel in any, should be regularized; or a single irregularity, like <gh>, should be removed. However, the immediate benefit of such a reform would be slight.

A new approach is called for if today's readers are not to be alienated, yet learners are to benefit significantly.

STREAMLINING

Cutting redundant letters

In the 1970s the Australian psychologist Valerie Yule found that many irregular spellings arise from redundant letters. These are letters which mislead because they are not needed to represent the sound of a word. Writers then cannot tell from a word's pronunciation which letters its written form requires, nor where to insert them, while readers are likely to mispronounce unfamiliar words containing them. A group within the Simplified Spelling Society therefore decided to explore which letters are redundant in English, and the effect their removal has on the appearance of the resulting 'cut' text. This Cut Spelling (CS) is now demonstrated.

Esy readng for continuity

One first notices that one can imediatly read CS quite esily without even noing th rules of th systm. Since most words ar unchanjed and few letrs substituted, one has th impression of norml ritn english with a lot of od slips, rathr than of a totaly new riting systm. The sential cor of words, th

letrs that identify them, is rarely afectd, so that ther is a hy levl of compatbility between th old and new spelngs. This is esential for th gradul introduction of any spelng reform, as ther must be no risk of a brekdown of rith comunication between th jenrations educated in th old and th new systms. CS represents not a radicl upheval, but rather a streamlining, a trimng away of many of those featurs of traditionl english spelng wich dislocate th smooth opration of th alfabetic principl of regulr sound-symbl corespondnce.

FURTHR ADVANTAJS

Savings

Th secnd thing one notices is that CS is som 10% shortr than traditionl spelng. This has sevrl importnt advantajs. To begin with, it saves time and trubl for evryone involvd in producing rith text, from scoolchildren to publishrs, from novlists to advrtisers, from secretris to grafic desynrs. CS wud enable them al to create text that much fastr, because ther wud be fewr letrs to rite and they wud hesitate less over dificit spelngs. Scoolchildren cud then devote th time saved in th act of riting (as wel as that saved in aquiring litracy skils) to othr lernng activitis. Simlr time-saving wud be experienced by adults in handriting, typng, word-procesng, typ-setng, or any othr form of text production. Th reduced space requiremnt has typograficl benefits: public syns and notices cud be smalr, or ritn larjr; mor text cud be fitd on video or computer screens; fewr abreviations wud be needd; and fewr words wud hav to be split with hyfns at th ends of lines. Ther wud also be material savings: with around one paje in ten no longr needd, books and newspapers wud require less paper (alternativly, mor text cud be carrid in th same space as befor), and demands on both storaj and transport wud be less. And th environmnt wud gain from th loer consumtion of raw materials and enriy in manufacturng and from th reduction in th amount of waste needing to be disposed of.

Targetng spelng problms

Less imediatly obvius is th fact that CS removes many of th most trublsm spelng problms that hav bedevld riting in english for centuris. Ther ar thre main categris: ther ar silent letrs, such as <s> in isle or <i> in business, wich ar so ofn mispelt eithr as ilse, buisness, or as ile, busness; th latr ar th CS forms. Anothr categry is that of variant unstresd vowls, as befor th final <r> in burglar, teacher, doctor, glamour, murmur, injure, martyr, wich CS neatly alyns as burglr, teachr, doctr, glamr, murmr, injr, martr. Thirdly ther ar th dubld consnnts, so ofn mispelt singl today, as found in such words as accommodate, committee, parallel(I)ed; CS simplifys these to acomodate, comitee, paralleld.

RULES OF CUT SPELLING

Cutting rules

These three problem areas of traditional spelling correspond to the three main rules of Cut Spelling (CS).

Rule 1 Letters irrelevant to pronunciation

About 20 of the 26 letters of the alphabet are sometimes used with no bearing on pronunciation at all. Some, like <e> in love, <gh> in though and <w> in answer, were once sounded, but fell silent centuries ago. Others were taken from foreign languages, like <ch> in yacht (Dutch), <h> in honest (French), and in psyche (Greek), but are always silent in English. Yet others were inserted by analogy (<gh> in haughty to match naughty, <l> in could to match would) or to show a dubious or imagined derivation (in doubt, <c> in scythe). Two vowel letters are often written when the pronunciation only needs one; thus <a> in measure, <e> in hearth, <i> in friend, <o> in people, <u> in build are all redundant. CS removes letters such as these from hundreds of often common words; most strikingly, CS eliminates that most grotesque of all English spelling patterns, the <gh>.

Rule 2a Unstressed vowels before <1,m,n,r>

Thousands of English words contain <-able, -ible> suffixes are mostly reduced to just <-bl>, turning eatable, edible into CS eatbl, edbl.

Rule 3 Doubled consonants simplified

Doubled consonants sound like single consonants, so the writer cannot tell when doubling is required: frequent errors are the inevitable result. CS simplifies nearly all of them, as in CS abreviate, embarass, omitd/comitd/benefitd, travld/ compeld and (by Rule 2) hopng/hoping for hopping/hoping. The main exceptions are disyllabic words ending in <y> and words ending in <ss>; furry, tinny, hiss, discuss therefore remain distinct from fury, tiny, his, discuss.

Substitution rules

The key feature of CS is that it removes rather than replaces letters. However, 3 simple substitutions are also made:

1 When



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 75

Weds 13 April 1994

Contents

E-Mail saves a man's life

PGN

Risks of powerful computers to the quality of science **Dan Ruderman**

Robot mower

Pete Mellor

God Grants Granite Gift to RISKS Punsters

Peter Wayner

The Soft Pork Underbelly of Efficient Markets

Peter Wayner

A creative, HONEST software disclaimer

Neil MacKay

E-mail problems

Andrew W Kowalczyk

Holiday Inn extra key requirements

Lance A. Brown

Fingerprinting & welfare

Mich Kabay

Re: More jail-door openings

Al Stangenberger

WAIS

Peter Wayner

Info on RISKS (comp.risks)

E-Mail saves a man's life

"Peter G. Neumann" < neumann@chiron.csl.sri.com> Sat, 2 Apr 94 13:24:39 PST

RISKS is always delighted to find cases in which the benefits of computing technology manifest themselves in a critical way. Here is such a case.

Jack Miller, a computer analyst from Paramus NJ, was experiencing severe chest pains and called his doctor, who put him on hold. As his condition worsened

to the point that he felt a strange coldness and could barely breathe, he was just barely able to type a piece of E-mail to coworkers: HELP. FEEL SICK.

NEED AID. Apparently he had intended to sent it just to a few nearby colleagues, but instead it appeared as an alert message on the screen of each of the 80 people in his department. Some of those who responded were trained in cardiopulmonary resuscitation, and his life was saved. [Source: an AP item in the San Francisco Chronicle, 2 Apr 1994, p.A1.]

✓ Risks of powerful computers to the quality of science

Dan Ruderman <dlr1002@cus.cam.ac.uk> Wed, 30 Mar 94 14:54 BST

Much of modern-day science relies on computer models for simulation and the testing of various hypotheses. The use of large scale simulations now permeates many fields, from the Monte Carlo algorithms employed by physicists and computer scientists to genetic mutation simulations performed by evolutionary biologists. As computers gain speed and data storage capacity, science's dependence on simulation will only increase.

I see two grave risks in this trend. First, the uses I mentioned above both rely heavily on having a "good" random number generator. But it is well known that even the best pseudorandom number algorithms posses large amounts of redundancy (and thus predictability) when viewed in high-dimensional spaces. But this is exactly the regime in which they are mainly used in science to simulate many-body dynamics. The second edition of "Numerical Recipes" discards its previous random number generator for a "better" one. Should all the thousands of simulations which used the first version now be redone?

The second potential danger is to the fundamental quality of scientific ideas. How long should you think about a problem before letting the computer take a brute-force crack at it for you? As computers become more powerful the temptation to stop thinking and start coding looms ever more prominently. As a high school computer nerd turned postdoc physics nerd, I am acutely aware of this seduction.

One aspect of this problem is that we may not think as hard as we used to. Another may be the predominance of work being on computer simulations rather than basic ideas. Since these simulations generally have many adjustable parameters, the space of possible exploration is huge, and not all of it relevant. This also makes the interpretation of results that much more difficult to grasp, since there is a large number of parameters to visualize. Pedagogically speaking, simulations should be used sparingly either to illustrate an idea or to perform an essential computation which cannot be carried out analytically. A proliferation of mediocre models with many arbitrary parameters can only spell disaster for the industry.

Dan Ruderman The Physiological Laboratory Cambridge CB2 3EG England

Robot mower (designed by Belgians, built by Swedes, driven by no-one)

Pete Mellor <pm@csr.city.ac.uk> Sun, 3 Apr 94 03:54:47 BST

The Daily Mail of 1st April 1994 carried a full-page report (p3) of a new design of mower called the Solar Turtle.

This is a little robot that runs around your lawn on wheels, cutting the grass ALL ON ITS OWN! The picture that accompanies the article shows a low-profile object about 3 feet long by 2 feet wide, elliptical in outline, and with its top surface sloping down from about one foot at the front to 6 inches at the back. (I am guessing: the exact dimensions are not given.) It is so light that "it can be carried by a child." It is also (mercifully!) almost completely silent.

Its flat upper surface is covered with an array of solar panels which provide it with sufficient power to trundle around even on dull days, and charge its little batteries so that it can keep going if it runs into a shaded patch of garden. Its maximum speed is 1.8 kph (slower in the shade). Three separate electric motors drive its two front wheels and rotating cutting blade. Since it is intended to operate continuously, the grass never gets a chance to grow. Therefore trimmings are very fine, and are simply left on the lawn as a mulch, so that no collector box is required, and it doesn't even require periodic attention from the gardener to empty it.

A single machine can look after 2000 sq. ft. of lawn. Price {pounds} 1,500 to 2,000 (still TBA). Manufacturers are Husqvarna of Sweden, and the inventor is Andre Coles (Belgian). So far, it has been demonstrated at the Spring Gardening Fair at Olympia, London. Look out for it next at the Chelsea Flower Show. It will probably go on sale next year. (British outlet: Husqvarna Forest and Garden.)

Risks? Well, what if it a) cuts your toe off, b) mows your prize dahlias, c) gets stuck, or d) gets nicked?

This is where the relevance of all this to the RISKS forum becomes apparent. For the Turtle is controlled by (you've guessed it, folks!) "an on-board computer [which] analyses conditions 500 times a second, enabling it to adapt to the amount of light, humidity and temperature, and to negotiate slopes and particularly overgrown patches."

- a) Safety (1): If it hits anything (tree, chair, foot) "a shock detector stops it in its tracks". The picture shows a sort of white band around the front edge, which is presumably a collision sensor. Since it moves "backwards and forwards a few feet at a time", it presumably has a similar sensor at the rear. Its sensor seems to be a few inches off the ground. Could it give a sleeping cat a short back and sides?
- b) Safety (2): It will not operate outside an area delimited by a buried "boundary cable". An "electronic sensor" detects the cable, and "tells it to turn back". The article does not go into this, but (IMHO) this is a serious marketing weakness. The photo shows the Turtle standing proudly in the foreground with a smiling and highly photogenic young lady (who obviously never got her hands dirty with a bit of weeding in her life!) lolling in a deck-chair in the background. The scenery includes (as well as the happy

Turtle user) about 50 acres of garden containing a lake, irregular patches of shrubbery, occasional trees, and artistically arranged lumps of rock. Even assuming the Turtle can negotiate the rocks, shrubs and trees without help, burying a boundary cable around that little lot must be a major logistical exercise.

- c) Reliability: This must depend on precisely how intelligent its program is. It can't simply stop when it hits a tree, so what does it do? Back up and charge again? Try a random turn? What happens if it hits your foot, and you then move out of the way? You can bet that even if you have more sense than to get in its way, your kids will have hours of fun trying to convince it that they are a tree! If it maintains a database of the terrain, this could seriously blow its tiny mind! :-) On the other hand, it must somehow avoid mowing the same little patch over and over again. Does it remember where it's been? (Software Engineering coursework assignment: "Design an algorithm using a pseudo-random number generator to ensure that a Turtle covers the whole of a piece of lawn 2,000 sq. ft. in area in a given time irrespective of the shape of the perimeter or the presence of interior obstructions." That should keep the students busy! :-)
- d) Security: If the Turtle is picked up, "a loud alarm goes off ... and is turned off only when an individual code is punched in. And it cannot operate outside the electronic boundary." ("I say, Alice! What's the code for this ****** Turtle? I can't turn the frigging alarm off!") Also, if it's *carried* outside the boundary cable, how does it detect this? Mmmm ...

After all that, risks to the public? Err ... getting fat through not having to mow the lawn? :-)

[There is a disclaimer in the Mail article which states that this is NOT an April Fool joke! :-)]

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq. London EC1V 0HB +44 (71) 477-8422, p.mellor@csr.city.ac.uk

✓ God Grants Granite Gift to RISKS Punsters

Peter Wayner <pcw@access.digex.net> Tue, 5 Apr 1994 15:25:20 -0400

The financial pages will be burning up with stories about a relatively small investment fund called "Granite." The fund was set up by "really smart guy" named David Askin to provide "RISK-free" investment in the the mortgage backed securities market. As early as middle March, Askin was pretty sure that his fund was still worth \$600 million. Now it may not be worth anything. Poof. In two weeks!

How could this happen? Everyone understands how money can disappear in the stockmarket. But, the Granite fund was different. Askin et al. used very sophisticated models to figure out which morgage-backed securities were cheap and which were dear. He would buy the cheap ones and sell out the expensive ones. Eventually, the market would drive the price of the cheap and dear

securities together. Then the fund would close out the position and make money based upon the original spread.

The great "strength" of plan was that it was supposedly interest-rate neutral. If the rates went up, then both the cheap and the dear securities would lose value in sync. They're both bonds so they tend to lose value as interest rates rise. So any loss in the value of the "cheap" securities that the fund actually bought was offset by a gain the value of the short investment in "dear" securities that fund sold short. The same process would work in reverse if interest rates dropped.

The main problem seems to be that no one was willing to buy any mortgage-backed securities as the bond rates went through the roof. The markets just froze. Plus, prices weren't behaving according to the very careful models that he originally created. Bam.

Interested parties should check out the various articles in the NYT (April 5, A1), Time magazine (cover), and other sources to find out more details.

The message for the comp.risks readers is the same old story of technical hubris that we've grown to love. But it is even better than almost any other case I've read about. People who use computers and mathematics on Wall Street usually have a stronger arrogance than those who use the computers to guide planes, run home security systems, run 911 systems or steer satellites. Why? Derivative securities, like those bought by Granite, are sheer creations of mathematicians. It is very tempting to believe that they're free from real-world problems like wind, noise, pets or other gremlins that keep plenty of engineers up late.

I've worked on Wall Street doing these sorts of things. The whole mathematical foundation of the work made things both very fun and very certain. I've always thought that mathematics was a very clubbish pursuit. The proofs were the rites of initiation. Once you made it in you could be sure that you and the other members of this club really did have a superior view of the world. Unlike the all-male, all-female, all-whatever clubs, you had actually _proven_ the truths you held up as self-evident. The mathematicians running these games are probably just as sure.

But, when the Bear putsch came to shove and the world tried to get out of the stock market at the same time, all of the mathematical models started breaking down. I can assure you that the people who bought into this fund probably thought that they were buying a sure thing. They had probably worked through the math themselves. There are probably lawyers combing the prospectus hoping that the Granite partners were so sure of themselves that they didn't put the usual disclaimers in the prospectus.

At this point, I'm wondering about of the dangers of using mathematics for a guarantee of even things mathematical. The theorem that all maps can be colored with four colors is widely known as the first example of computer-based proofs. Many people don't remember that the theorem was originally considered settled and true back at the turn of the century. People believed the "proof" for several decades. Then someone stumbled upon a loophole and it became famous again.

--Peter "I will build my Church/Turing theorem on this Granite" Wayner

★ The Soft Pork Underbelly of Efficient Markets

Peter Wayner <pcw@access.digex.net> Thu, 31 Mar 1994 23:30:20 -0500

The Under Pork Belly of Efficient Markets, or How to Launder Money Using Cattle Futures

The great promise of electronic networks and virtual communities is a collection of very efficient markets. In the future, information will be moved, products will be sold and trades will be executed in a blink of an eye. This efficiency is usually considered to be a pretty good thing by everyone in business, in economics or in line at the video store. The underside of this efficiency, though, is a blurring of the line between legitimate and illegitimate business.

A good way to understand this effect is to study the case of how to launder money using the futures markets. Laundering money is an age old problem for people who want to move funds from person A to person B without leaving a suspicious trail. Cash is the nieve approach and it has plenty of problems: it is bulky, it can be lost or stolen, and most importantly it often leaves people asking "Hey, where did that come from?"

The futures markets, though, make it simple to move funds in a way that is indistinguishable from ordinary commerce. If it is done correctly, the recipiant, person A, looks like a lucky stiff or a market savvy investor. Person B is usually out of the picture or out of luck. The same games can be played with almost any other market, but futures markets are so efficient that the process is actually feasible and easy to do.

The basic transaction in futures is to buy or sell a contract for the delivery of x pounds/barrels/tons/feet of some commodity at y dollars/yen/marks etc. If you buy a contract, then you're obligated to actually cough up y dollars when the contract comes due. Most people don't hold on to the contracts long enough for them to actually take delivery. They sell another contract and the futures market maintains a clearing house that is responsible for matching up the contracts and cancelling them out. It's a great system. Very efficient and very useful for farmers, manufacturers and others who actually produce and consume commodities.

Futures markets are great for laundering money, though, because they can generate big losses or big gains in a short amount of time. It is quite possible for \$100 to turn into a \$5000 gain overnight. The downside is that it can often turn into a \$5000 loss in the same amount of time. In fact, the market is a zero sum game. If you make n dollars, then there is someone out there who just lost n dollars. The sum total of the losses and the winnings equals zero.

This zero sum nature is the key to laundering the money. Person A and Person B get together and guess that the price for a commodity is going to go up. That

means that who ever buys a contract will make money. So Person A, the intended recipient buys a contract and Person B sells a contract. If they're right, then Person A gets the money and Person B loses the same amount.

Bingo. The money moved from B to A and no one can trace how it got there. Person A looks smart or lucky and Person B looks out of luck. There was no direct connection between the two. There are thousands of other people out there winning and losing money at the same time. The marketplace's central clearing house arranges it so each wins and loses their rightful share.

You may wonder why B bothered to sell a contract and lose money. This is the safeguard against guessing wrong. No one is correct all of the time. Even the people who try and rig the markets and corner them get burned as often as they succeed. The best investors in the futures markets, the ones who make money time after time, are the arbitrageurs. They spot inefficient pockets and try and remain neutral to the overall shifts in the market.

Person B sells the contract so that if the market goes down, i.e., the wrong way, then A and B together have lost no money. It's a zero sum. Now they just have to play the game a bit longer or for stakes that are twice as high. You can think of the process as flipping a coin until you have encounter a heads.

Ideally, you play this game with two players with relatively deep pockets. This means that A can cover the short term loses. This is a bit of a disadvantage because many money laundering operations must move cash from the rich to the poor. You can cover up this problem by using the same broker for A and B. The broker executes the trades and then assigns the winning trade to A and the losing trade to B. They fill in the order books after the fact.

Using the same broker for A and B can be problematic because it may look too suspicious if the mirrored trades appear on the same ledger. The beauty of this system is that it can look quite indistinguishable from normal business practices. Many companies actively enter the futures markets to hedge themselves against foreign currency movements. Others actively enter the futures markets to guarantee themselves a good supply of their raw materials.

The essential point of this lesson is that fast, efficient markets make it possible to move money easily. The futures markets were designed so that is no real other half to every trade. It's literally you against the world with every trade. The RISKS, of course, is that accountability can vanish as the size of the crowd grows to be as big as the world. There is no way to catch up with this. The futures market are so great because there is no need to deal one on one.

The effects of speed are not only apparent in big financial markets. Credit cards and overnight delivery are a dangerous combination. You could steal cards, order a fortune of stuff, arrange for it all to be delivered overnight and then jump town quickly before people notice the card was gone. Suddenly, merchants must deal with the fact that something that used to be complete legitimate (exchanging cash for goods) is now a potential theft.

Of course, there are other crimes that lose their edge. It is much harder to escape the law by heading to a new town. Computerized fingerprint files are

very, very efficient.

I think everyone felt that perfect, computerized markets would bring about the right mixture of accountability and efficiency. It would be a perfect mixture of Big Brotherly scrutiny would take care of everything. Every trade, after all, is recorded in the futures market. Yet, the best mechanism for anonymous fund transfer yet discovered exists here in the midsts of all of this record keeping, legal scrutiny and oversight.

✓ A creative, HONEST software disclaimer

<NMACKAY@VM2.YorkU.CA> Thu, 31 Mar 94 21:11:41 EST

To add one more to your creative software disclaimers; I read this one in WIRED magazine issue #2.01. It is reprinted without permission. It concerns Haventrees Software's EasyFlow program.

If EasyFlow doesn't work: tough. If you lose millions because EasyFlow messes up, it's you that's out the millions, not us. If you don't like this disclaimer: tough. We reserve the right to do the absolute minimum provided by law, up to and including nothing. This is basically the same disclaimer that comes with all software packages, but ours is in plain English and theirs is in legalese. We didn't want to include any disclaimer at all, but our lawyers insisted.

Certainly clarifies their position. In a strange, twisted, punkish kind of way I admire them. :-)

Neil...

✓ E-mail problems

Andrew W Kowalczyk <AKOWALCZ+aLIFDR1%Allstate_Corp+p@mcimail.com> Fri, 1 Apr 94 19:46 EST

With all the tribulations you have gone through in trying to mail stuff properly through the various E-Mail systems I thought you might enjoy this joke that was related by columnists Nicholas Petreley and Laura Wonnacott in the March 28, 1994 issue of InfoWORLD:

A fellow goes into a bar and says to the bartender, "Hey, I just heard this great E-mail gateway programmer joke."

The bartender replies indignantly, "Now, wait a minute. I used to be a gateway programmer. See that guy at the end of the bar? The guy at the other end? Those two guys at the table over there? They are all gateway programmers. Now, do you still want to tell that joke?"

And the fellow says, "Well, not if I have to explain it five times."

Andy Kowalczyk, Allstate Life Insurance Co., 1415 Lake Cook Road P2A, Deerfield IL 60015-5213 (708)317-6206 AKOWALCZ+aLIFDR1%Allstate_Corp+p@MCImail.com

Holiday Inn extra key requirements

"Lance A. Brown" <lab@biostat.mc.duke.edu> Thu, 31 Mar 1994 23:50:59 -0500

Last weekend, March 27th I checked into a local Holiday Inn for an overnight stay and was given only 1 credit card style mag-stripe key. A few hours later I went back to the desk and requested another key for my wife. The clerk asked for my name and room number, pulled something up on her computer, swiped a key through a card read (writer?) and handed it to me. No photo ID or other ID requested.

I asked if it is standard to not request ID for extra keys and was told that is true. I then asked her if she realized anyone could get a key just by knowing the name of a person and what room they were in. She seemed quite startled by this.

The RISK is quite obvious.

Lance Brown lab@biostat.mc.duke.edu

Fingerprinting & welfare

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM> 01 Apr 94 07:26:21 EST

>From the Associated Press newswire via Executive News Service on CompuServe (GO ENS):

Welfare Fingerprints, By KATHLEEN HOLDER, Associated Press Writer

SACRAMENTO, Calif. (AP, 31 Mar 1994) -- Expanding the use of fingerprinting to flush out welfare cheats, Los Angeles County will soon start taking the prints of applicants for federal dependent children benefits.

Officials said the requirement, which won state approval Wednesday, will be the nation's first use of fingerprinting to prevent fraud by applicants for Aid to Families with Dependent Children, the main federal-state welfare program."

The author explains the background and details. Key points:

- o electronic fingerprint scans of applicants are stored in computer database.
- o fingerprint taken as unique authenticator of identity.
- o Los Angeles has been using these techniques since 1991 for state general

assistance.

- o Needed and received a waiver from federal govt to add requirement to federal regulations for AFDC.
- o These techniques will be implemented state-wide if they work.
- o Several advocates for poor people's rights object to the stigma of fingerprinting.
- o "In the first six months after Los Angeles County began running fingerprint checks for general assistance in 1991, the county reported cutting its costs by \$5.4 million, or more than half."
- o "More than 3,000 people lost their aid for suspected fraud, and more than 200 applicants were denied assistance because they refused to submit their fingerprints."

Michel E. Kabay, Director of Education, National Computer Security Assn

★ Re: More jail-door openings (Markson, RISKS-15.73)

Al Stangenberger <forags@nature.Berkeley.EDU> Fri, 1 Apr 1994 20:43:04 -0800

> a jail in Marin ...

There's something wrong with this -- Polly Klaas's accused killer is housed in Santa Rosa, Sonoma County. Not Marin. I don't think Marin's new jail is finished yet.

Al Stangenberger, Dept. of Env. Sci., Policy, & Mgt., 145 Mulford Hall - Univ. of Calif., Berkeley, CA 94720 forags@nature.berkeley.edu (510) 642-4424

WAIS

Peter Wayner <pcw@access.digex.net> Fri, 8 Apr 1994 13:36:38 -0400

Q: What is WAIS?

A: It stands for Wide Area Information Server. It's a pretty popular standard for accessing text based information on the Internet. Anyone can use readily available software to create an index for a collection of texts and then make this available to the world on the Internet.

Q: How do you use it?

A: Get the right software, choose some data bases, type in some keywords and press the button. WAIS will come back with a list of documents and their matching quotient. You can then choose to read the entire text of the documents.

Q: Why would RISKS readers care about this?

A: Comp.risks digests are indexed with a WAIS server. You can type in "plane crash" and get more than enough information to keep you wondering about one, two and three engine planes that fly-by-wire using code written in Fortran and encrypted with Clipper to prevent terrorist hackers.

Q: How can I get the software?

A: There are many different ways to access WAIS. Many GOPHER servers offer it as an option. You won't even leave GOPHER to type your query.

You can also use TELNET to "quake.think.com" and log in as "wais" to use their link. The interface isn't great, but it is not bad.

The best options seems to be to get a copy of the specialized software written for different platforms. One package, which I've used occasionally is called "MacWAIS." It is available via anonymous ftp from ftp.tidbits.com. You need to have a Macintosh computer with an Internet connection using MacTCP to use this. There are other copies for NeXTs, PCs and other machines at ftp.think.com in the "/wais" directory.

Q: Are there any tricky parts?

A: Well, it is pretty easy in some respects. You just type and go. I've occasionally had trouble getting a good list of servers that are available. The WAIS folks were clever enough to make it possible to use WAIS to search through the lists of servers. You just type in some keywords and back comes a list of servers that have that keyword in their description.

So, if you want to access RISKS, try searching the directory of servers for the keyword RISKS. Once you find it, you will be able to save the result on your machine and it will automagically know about the RISKS server.

Another solution is to search through the directory of servers using ".src". Several people have recommended this to me, but I've had trouble getting it to work well for a number of reasons. First, it only searches the description string of each server. If the author/creator of the server was parsimonious with the description, then you might not even find the world ".src" in there. I've tried all kinds of keywords, but I've often felt like there are still many sources out there that I just can't find.

This problem may be fixed or solved by now. (Please write if it has.)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 76

Monday 18 April 1994

Contents

"Friendly Fire" --- U.S. F-15s take out U.S. Black Hawks

The Green-Card Flap

PGN

Data-storage technique provides copy protection Meine van der Meulen

Yet another example of software modification risks

Jim Dukelow

Re: Risks ... to the quality of science [randomness]

Steen Hansen

MIT student arrested for BBS used for pirate software

Fredrick B. Cohen

Credit-Card Fraud

Greg Philmon

NII and the US Card

Bill Murray

Reckless Baby Bell Marketing

Alan Miller

Re: P.R. China Computer Security Rules

Tom Albertson

Dan Sorenson

Delayed Dial Tone causes unintentional 911 calls

Chonoles Michael Jesse

Information resource

Michael Enlow

Info on RISKS (comp.risks)

✓ "Friendly Fire" --- U.S. F-15s take out U.S. Black Hawks

"Peter G. Neumann" < neumann@csl.sri.com> Mon, 18 Apr 94 14:51:28 PDT

[This item may be old news now, but is included for the archives.]

Despite elaborate precautions designed to prevent such an occurrence, two American F-15C fighter planes shot down two U.S. Army UH-60 Black Hawk helicopters in the no-fly zone over northern Iraq on 14 Apr 1994, in broad daylight, in an area that had been devoid of Iraqi aircraft for many months. One Sidewinder heat-seeking missile and one Amraam radar-guided missile were fired. The fighters were operating under the communication control of an AWACS plane, which was the first to detect the helicopters, and instructed the F-15s to check the situation out. The helicopters were carrying U.S., British, French and Turkish officers from the U.N. office in Zakho, in northern Iraq, and were heading eastward for a meeting with Kurdish leaders in Salahaddin. Both towns are close to the Turkish border, well north of the 26th parallel that delimits the no-fly zone. All 26 aboard were killed.

Both helicopter pilots apparently failed to perform the routine operation of notifying the AWACS plane after their last takeoff. Both helicopters apparently failed to respond to the Identification: Friend or Foe (IFF) requests from the fighters. Both fighter pilots apparently did not try voice communications. A visual flyby apparently misidentified the clearly marked ("U.N.") planes as Iranian MI-24s. Furthermore, a briefing had apparently been held the day before for the appropriate personnel of all of those aircraft (F-15s, UH-60s, and AWACS). There was speculation as to whether the pilots of both helicopters might have neglected to turn on their transponders, or whether the frequencies were set incorrectly, or whether both transponders failed (or perhaps some hybrid scenario). There was speculation that the fighter pilots did not try all three of the IFF modes available to them. There was also speculation that the Black Hawks may have visually resembled Russian helicopters because they were carrying extra external fuel tanks. But the AWACS plane personnel should have been aware of the entire operation, because they were acting as battlefield coordinators.

Perhaps someone panicked. An unidentified senior Pentagon offical was quoted as asking "What was the hurry to shoot them down?"

[Sources: various press reports in The New York Times and other papers, 15 Apr 1994 and 18 Apr 1994.]

"Friendly fire" (also called fratricide, amicicide, and "misadventure") is not uncommon. An item by Rick Atkinson in The Washington Post (15 Apr 1994) noted that 24 percent of the Americans killed in action -- 35 out of 146 -- in the Persian Gulf war were killed by U.S. forces. Also, 15 percent of those wounded -- 72 out of 467 -- were similarly victimized. RISKS noted earlier the British Warrior armored vehicles that, mistaken for Iraqi T-55 tanks, were zapped by U.S. Maverick missiles, killing 9 men and wounding 11 others. Atkinson's article noted that this is an old problem, citing a Confederate sentry who shot his commander, Stonewall Jackson, in 1863, during the Civil War; an allied bomber that bombed the 30th Infantry Division after the invasion of Normandy in July 1944; and a confused bomber pilot who killed 42 U.S. paratroopers and wounded 45 in the November 1967 battle of Hill 875 in Vietnam. The old adage was never more appropriate: With friends like this, who needs enemies?

The Black Hawk incident also brings back memories of the Soviet shootdown of the Korean KAL 007 flight and the Vincennes' shootdown of an Iranian Airbus.

The Green-Card Flap

"Peter G. Neumann" < neumann@csl.sri.com> Mon, 18 Apr 94 15:12:17 PDT

RISKS received a huge amount of mail relating to the husband-and-wife Phoenix immigration-law-firm, Canter & Siegel. Offering their legal services, they posted an advertisement on 5000 newsgroups, and gave information on a forthcoming lottery that will give out 55,000 green cards (granting permanent residency in the United States). C&S received at least 30,000 responses, mostly protesting their use of the Internet for advertising.

Internet Direct suspended the C&S account for violation of the customer service agreement. I.D. had to put up with the thousands of pieces of objections. [This gives a new meaning to OBJECT-oriented E-mail.] C&S threatened to sue for I.D. for \$250,000 for the lost responses. At least one site crashed repeatedly because of mail saturation.

This reminds me once again of all the varied problems that I have with the fly-by-night it's-not-quite-the-Internet providers. One of them rejects mail after you hit your quota of external mail for the month. Some include the entire mailing list on each RISKS mailing, as noted earlier. Many do not permit FTP, but offer thousands of users the opportunity to invoke the almost-costfree availability of my pro-bono but not timefree services. Is regulation an answer? I shudder at the thought.

I cannot begin to summarize the RISKS mail on this subject, and certainly would risk losing most of our subscribers if I ran the whole collection. The issues include the usual stuff about whether the no-advertising policy even exists, whether it is a per-newsgroup question or an Internet policy question, who actually controls the Internet, and all those topics familiar to RISKS folks. Perhaps we are waiting in expectation of the ultimate scam from New Haven, which might be considered a violation of Con-netiquette.

Data-storage technique provides copy protection

<MEULEN@tno.nl> Thu, 14 Apr 1994 13:26 +0100 (MET)

Data storage technique provides copy protection

Summarized and translated from "Intermediair", 1 April 1994, Vol. 30, Nr. 13, p. 35.

Universities of Plymouth (in the U.K.) and Washington DC developed a technique to write five times as much information on magnetic media as floppy discs or bank cards. The magnetic layer is composed of small magnetic particles. Every bit is "remembered" by polarising several thousands of them in the same direction. This is done to overcome noise, due to the random orientation of the particles. The new technique only uses a fifth of the number of particles used in conventional techniques. It reads the information on the medium

directly after writing it. By comparing the real magnetisation with the expected one, a chip determines the deviations in the medium. Based on that, information about these deviations is also written on the medium. Later, this enables flawless read out. An extra feature of this technique is that the information about the deviations is unique for every medium, comparable to a fingerprint. This means that when a bank cheques this fingerprint, it can detect fraud copies of bank cards.

Meine van der Meulen TNO-Industrial Safety Department meulen@tno.nl

Yet another example of software modification risks

<js_dukelow@gate.pnl.gov>
Fri, 15 Apr 1994 13:16 -0800 (PST)

The following is a slightly edited version of a report from the latest issue of the Department of Energy Operating Experience Weekly Summary, which is a vehicle for rapid dissemination to other DOE organizations and contractors of occurrences at DOE facilities.

"On January 17, 1994, the earthquake in Southern California caused widespread power outages in the western portion of the United States, and commercial power was lost at a DOE chemical processing facility. When commercial power was lost, a standby diesel generator automatically started and supplied power to critical loads. During a power transient caused by starting a large load on the diesel generator, four electric motors dropped off line and did not respond to a start command even though individual controllers indicated a ready-to-start condition. Facility personnel had to completely de-energize and then re-energize the motor controllers before the motors could be re-started.

"After commercial power was restored, facility personnel determined that the porblem could not be duplicated for partially loaded generator conditions or with commercial power supplying the standby motor control center. Investigators determined that all the affected motors were connected to the same standby motor control center which was equipped with new digital motor protectors. Facility personnel developed a series of test procedures to determine the cause of the problem. After extensive testing, they determined that the motor protectors developed a software lockup after a power transient. During a simulation of the loss of commercial power, investigators determined that there was a correlation between voltage swings caused by starting a large load on the standby generator and the software lockup of the motor protector. The motor protector lockup resulted in the motor tripping off and not restarting until control power was removed and re-applied.

"Facility personnel contacted the motor protector vendor with the results of the tests conducted at the facility. Vendor personnel confirmed the test results and reported that they had isolated the problem to specific units with firmware version F3, introduced in the fourth quarter of 1991. The vendor reported that units manufactured from 1987 through the third quarter of 1991 were not affected.

"The vendor also reported that the units operated properly if the control voltage is maintained within plus or minus ten per cent of nominal voltage. If the control voltage surges beyond this range, the motor protector may trip the motor and require a power down to reset itself. The vendor offered to modify the affected units to eliminate the power reset after a voltage surge.

"DOE facility personnel are advised to inspect their facilities for the suspect motor protector and take appropriate corrective actions."

The risk associated with this event is that a software modification in 1991 rendered the standby electrical power system partially unable to fulfill its safety function. The root cause of this situation was that software engineer(s) involved in this modification (which was perhaps the initial digitally-controlled version of this component) were not fully aware of the actual operating environment (in this case, voltage swings greater that +/- 10% when the standby power system was doing what it was designed to do) of the digitally-controlled component.

Jim Dukelow Battelle Pacific Northwest Laboratories js_dukelow@pnl.gov

★ Re: Risks ... to the quality of science (Ruderman, RISKS-15.75)

Steen Hansen <steen@kiwi.swhs.ohio-state.edu> Thu, 14 Apr 94 08:09:46 -0400

Some years ago I upgraded the operating system of a minicomputer. A few weeks later a faculty member became very upset: his research results had changed. Apparently the upgrade changed the random-number generator, which made his statistical programs give a different result. He demanded the original generator be put back in again.

Steen Hansen, Computer Specialist, Ohio State University hansen+@osu.edu (614) 292-9317 (Stores/Food: Tue/Thu/Fri) (614) 292-5174 (Dentistry: Mon/Wed)

✓ MIT student arrested for BBS used for pirate software

Fredrick B. Cohen <fc@Jupiter.SAIC.Com> Fri, 15 Apr 94 17:11:42 PDT

An MIT student was arrested today for having a BBS at the school that was used by the participants to store and fetch commercial software. This one made the national news because of the promenance of the institution and the information superhypeway, but this sort of arrest has been going on for years in the "hacker" bulleting boards of the US. There is now a substantial history of these operators being convicted, but I have to question whether MIT should be arrested for allowing the BBS to reside on its computers. After all, if the BBS superuser can be arrested for unknowingly having the software on their BBS, why can't the institution be arrested as well?

But the issue goes far deeper than this. At its core, we have the multitudes of people trying to tell us that the information superHW should have public access points and public spaces, but what happens when a public space is used for crime? The criminal is not arrested; instead, the person who provided the space is arrested. If we are to have public space on our info superHW, we had better stop arresting those who provide it for the crimes perpetrated in it. Otherwise, there will be a chilling effect on those who would provide it.

How does this relate to RISKS? It should be obvious. If you have a party, and someone who attends commits a crime, you may be sent to jail for it. No precedent? Huh! If someone is drinking at your house or bar, and you fail to prevent them, and they drive away and get in an accident, you may be liable.

I anxiously await your responses on the policy issues at play here. FC

Credit-Card Fraud

Greg Philmon <philmon@netcom.com> Thu, 14 Apr 1994 05:50:38 -0700

A friend recently applied for a credit card from a major issuer. Later he received a call from the bank informing him that his card was in a batch that was stolen somewhere along the delivery route. Over \$4000 had been charged to his card in a 24 hour period.

This was once quite common. However, most card issuers now use an automated system to "activate" the card. Usually it involves dialing an 800 number and entering some "secret" information (e.g. your birth date, ssn, etc).

As it turns out, my friend's wife had received a phone call from someone claiming to work for the issuer. He said that they wanted to verify his application and asked for the his full name and SSN, which she gave.

The automated authorization system of this issuer asks for the last four digits of your SSN.

I'm really curious what sort of success rate was achieved by the thieves. Did they get fifty percent of the card owners to give their SSNs? More?

Greg Philmon | philmon@netcom.com | CIS: 71161,3445 | MCI: 588-5358

NII and the US Card

<WHMurray@DOCKMASTER.NCSC.MIL> Sat, 16 Apr 94 16:06 EDT

Last week in the security track of the CardTech/SecureTech Conference, I heard a presentation by a representative of the U.S. Postal Service on the "US

Card." This is a piece of the national information infrastructure intended to mediate all government services to and controls over the citizen.

It will contain health care data, financial data, tax data, and identity data. It will contain a private key (digital signatures only), a PIN, and other identifying data. (While emphasizing that "open to new applications" was a requirement of the system, he was silent on arrest record, voter registration, gender preference, and previous condition of servitude.)

Use of the card will be "voluntary." The government is doing this for us because it will enable them to give us better service, because the citizens require "one card," and to protect us from the "twenty million 'little brothers'" that we now recognize as the "real threat to our privacy." (He did not claim that this would protect us from terrorists, child molestors, drug dealers, or religious cults.) (All of this was delivered with a perfectly straight face and without challenge from the audience.) Of course if we do not like it, we can do away with it, right?

The official stated that the Postal Service is prepared to issue a ahundred million of these cards within months of getting the go ahead.

Along with the net, "voluntary" fingerprinting of the poor, CLIPPER, and the FBI's digital telephony initiative, what more could any citizen, not to say government, ask for? Law and order is just around the corner.

Aren't you glad to hear that Orwell had it all wrong?

William Hugh Murray, Information System Security, 49 Locust Avenue, Suite 104
New Canaan, CT 06840 1-0-ATT-0-700-WMURRAY; WHMurray@DOCKMASTER.NCSC.MIL

Reckless Baby Bell Marketing

Alan Miller <millera@mcs.com> Thu, 14 Apr 1994 11:04:55 -0500 (CDT)

The following is most of a letter I sent to my local Baby Bell recently after receiving a marketing letter aimed at increasing calling card use. I think the risks of the mailing are fairly obvious from the letter... ajm

I simply wanted to inform you that I was disturbed to find in my mail an unexpected letter from you that contained my Ameritech Calling Card PIN. My objections to this letter are as follows:

- 1) Since I was not expecting the letter, if it had been removed from my mailbox or the U.S. Mail before I received it I would have had no way of knowing that something was wrong until I got my next phone bill (complete with calls I hadn't made).
- 2) Increasing the possibility of delivery problems, the address on the envelope was, if not wrong, at least very nonstandard. In particular, it had two different forms of the town name, both on separate lines. If something this easy to catch made it through

processing (presumably for many letters), what other errors might do the same? My monthly phone bill is properly addressed.

- 3) [Given a name and address, anyone with reason (PIN possession) can get my phone number]
- 4) [I can call customer service and get a new PIN assigned if necessary]
- 5) Finally, the presence of my PIN on the letter is not necessary on what is obviously a letter intended to increase awareness of calling cards. A note that I could contact Customer Service would have served just as well, without any of the security risks.

Since card number theft is a serious and reportedly increasing problem, I am surprised to see Ameritech sending mailings that include information that consumers are told to guard carefully. If this mailing does result in an increase in calling card fraud, is Ameritech intending to absorb all fraudulent charges resulting from the careless distribution of PINs? The letter also makes me wonder about the security of my account with Ameritech. How simple would it be for someone looking for the ability to make a few free phone calls to simply look up and write down a few number+PIN combinations?

★ Re: P.R. China Computer Security Rules

Tom Albertson <tomalb@microsoft.com> Wed, 13 Apr 94 09:40:10 PST

Our contacts with the PRC government say that these rules do not exist. While this may be only a denial of something still in the works, its quite possible these are the work of someone with a regional axe to grind. Would you be willing to put me in touch with the anonymous poster, or would you debunk this on your own? If the rules are not legitimate, I don't think it was correct to post without some corraboration (I thought the unwritten rules of journalism called for two reliable sources for unsubstantiated materials?)

Tom Albertson tomalb@microsoft.com PH 206-936-6764

Re: P.R. China Computer Security Rules

Dan Sorenson <viking@iastate.edu>
2 Apr 94 07:32:12 GMT

Note: this is somewhat political in nature, but I believe the RISKS are known to all in any position of responsibility or power.

China opens the "Golden Bridge" to the Internet, and I see China still writes laws like the following:

>Article 2. The computer information systems referred to in these regulations >are man-machine systems, composed of computers and their allied and

>peripheral equipment and facilities (including networks), that collect, >process, store, transmit, and retrieve information according to prescribed >goals and rules of application.

And in all likelihood this law would cover a supermarket scanner and cash register. I'm not surprised. Read any bill before Congress here in the USA and you will find a similar lack of understanding, broadness of definition, and lack of detail.

Perhaps a better example shows up daily in the newsgroups rec.guns and talk.politics.guns, where laws as passed are picked at and it is generally determined that the law outlaws anything not specifically mentioned as exempt.

The RISK? When people write the rules we have to live by, often times the spirit of the rule is lost in the letter, and the RISK of abuse is increased. One has to wonder at some of the latest anti-discrimination laws that wouldn't allow, say, a trucking company to not hire an applicant in an iron lung. I'm sure you can see your own pet versions of laws gone awry by creative interpretation. Finally, we're left with the axiom "You can't make it foolproof because fools are so clever." I submit that fools, lawyers, and government share this same affliction, and if we're not careful we shall as well, no matter our level of power over others.

* Dan Sorenson, DoD 1066 viking@iastate.edu z1dan@exnet.iastate.edu *

Delayed Dial Tone causes unintentional 911 calls

Chonoles Michael Jesse <chonoles@acc1.acc.vf.ge.com> Fri, 1 Apr 94 17:49:08 EST

Mostly, the problems with telephone numbers in the form x91-1xxx is the possibility that the first digit was ignored because of a delayed dial-tone.

If the exchange is busy, and there are many people calling, the exchange may not have enough "digit registers" to allocate. Then there is a delay before the dial-tone appears. [Similar to what happened with the rock-concert ticket giveaway and on Mother's day, etc.]. Since most callers often don't listen for the dial-tone and dial anyway, dialing a number in the form of x91-1xxx might get them 911.

As the number of central office codes (COCs), (the first three digits of a 7-digit number) is used within an area code increases, then these x91-1xxx numbers need to be allocated. The central offices that handle the x91 COCs need to have extra "digit registers' to lessen the chance for this problem.

Michael Jesse Chonoles chonoles@acc.vf.ge.com mjc@eniac.seas.upenn.edu

[This is another variation on an old problem addressed in many past issues of RISKS. PGN]

★ Seeking lit ref: we trust calculators over ourselves

Mike Crawford <crawford@scipp.ucsc.edu> Sun, 17 Apr 1994 21:48:54 -0700

I seek a literature reference. The usual methods have failed so far - perhaps someone can give me even an author, more precise subject or partial title words?

I will persist by looking up the references in papers referring to student use of calculators, but maybe this will ring a bell with you?

There was a study done, perhaps in the seventies, of the human tendency to trust machines rather than our own judgement.

Subjects were given calculators, and pages of simple arithmetic problems. The calculators were wedged so that they gave incorrect answers sometimes. Even though the problems were simple enough that the subjects could figure them out in their heads, the study showed that people will trust the machine even though our own judgment tells us that the machine is wrong.

I want to use this as a reference in a paper I am writing on computer network security, and another I am writing about why high-aenergy physicists should not be so trusting of their results if they have been subjected to extensive processing by complex, and poorly understood computer programs.

Thus, network administrators trust security software even when security experts tell them it is easily penetrable, and physicists trust the results of their calculations even when software experts tell them that their software is bogus. ;-) (C'est Moi! My own advisor does not believe me when I tell him the results of my own work are wrong. After all, they _were_ calculated on a computer!)

Author of the Word Services Apple Event Suite.

Mike Crawford crawford@scipp.ucsc.edu Free Mac Source Code:

ftp sumex-aim.stanford.edu | get /info-mac/dev/src/writeswell-jr-102-c.hqx

Information resource

Michael Enlow <m_enlow@enlow.com> Wed, 13 Apr 94 00:26:45 -0700

We wanted to let you know about some great info we are making freely available on the Internet.

My name is Michael Enlow. I am a retired private/legal investigator and author of several books regarding private investigation/electronic surveillance technology.

I wish to extend my services to the Internet to share and exchange information on security and privacy protection issues. We are making a lot of very informative info available FREE on the Internet. This includes back issues of my newsletter "Inside Secrets", my schematics and plans, resources, guides,

and other information.

For details on accessing these FREE services, send an e-mail message to INFO@ENLOW.COM you can also FTP to ENLOW.COM or FTP.ENLOW.COM, and login as anonymous (put your email address as the password). There is a listserver in place to send you files if you do not have access to FTP. Your comments and suggestions are welcome.

Thanks for your time.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 77

Tuesday 19 April 1994

Contents

- Risks ... to the quality of science: Clifford Truesdell **Michael Tobis**
- Dial-in Electric Meter Readings Sans Safeguards Scott Rose
- Stun belts -- who has the remote? Jak Kirman
- Risks of Data Compression Joe Decker
- TV Guide Contest

Agris Taurins

- Re: MIT student arrest **Dwight Silverman**
 - Sidney Markowitz
- Re: Green-Card Flap [Risks, Lawyers] **Ed Clarke**
- "Naissance d'un virus" by Ludwig/Condat Rob Slade
- IFIP SEC '94 Program Willis H. Ware
- Info on RISKS (comp.risks)
- ★ Re: Risks ... to the quality of science (Ruderman, RISKS-15.75)

Michael Tobis <tobis@skool.ssec.wisc.edu> Mon, 18 Apr 94 22:27:56 -0500

This issue was addressed in a remarkable essay by the eccentric and curmudgeonly fluid dynamicist Clifford Truesdell. The essay is called "The Computer: Ruin of Science and Threat to Mankind", in _An Idiot's Fugitive Guide to Science, Springer Verlag, 1984. If the title is not temptation enough, the following is a list of subheadings in the essay, capitalization intact:

1. Spatial Flight would have been Impossible without Computers.

- 2. Spatial flight would have been impossible without the Classic Equations of Motion
- 3. Calculation without Classic Standards is Dangerous. A Computer is Incapable of Setting its own Standards.
- 4. Computers have Harmed Science Already.
- 5. Mathematics is the Science of Infinities. Computation is Essentially Finite.
- 6. Computers Bring Power and the Abuses of Power. Advocates of Computing Seek to Destroy Mathematics.
- 7. Computing Promotes Factual Fraud. It has Harmed Experimental and Applied Science in the Past and is Copntinuing to do so. By its Emphasis on Application of the Already Known, it can Delay Basic Discovery and thus Reduce the Field of Applications in the Future.
- 8. Classic Theories used Inductive and Deductive Models. Computing Encourages Floating Models.
- 9. Computing Promotes Logical Fraud. Computers Programmed to Confirm False Theory can Destroy Mankind.
- 10. Summary: Computers are Here to Stay. They Endanger Thought, Language, Science, and the Survival of Man. Like any other Dangerous Tool, they should be Put under Strict Controls.

[OK, perhaps it's a bit overdrawn, but I think anyone who intends to use computers to model nature should have a look at this remarkable jeremiad. mt]

✓ Dial-in Electric Meter Readings Sans Safeguards

Scott Rose <rose@cs.wisc.edu> Tue, 19 Apr 1994 09:00:25 +0100

My electric utility-- Madison Gas and Electric-- has embarked upon a new meter-reading scheme that seems not to have been given a whole lot of thought.

Many of the electric meters in my neighborhood are not accessible from outside the house, so the chances of meter-reader getting the data on a particular visit are quite low in this era of double-income households.

In the old scheme, the meter-reader left a business-reply postcard after ostensibly determining that the customer wasn't home to allow access to the meter (in practice, the meter reader just leaves the card without notice, apparently having determined that the route can be finished more quickly without those pesky delays associated with actually determining that the customer isn't home, but that's a flame for another forum). The meter-reader fills in the meter number section of the card-- a six-digit number that uniquely identifies the meter-- the customer fills in the usage section of the card and drops it in the mail, and MG&E picks up the roughly \$.30 tab for the reply card postage.

The new scheme is similar, except that instead of leaving a mail-in card, the meter-reader leaves a phone-in card. Customers each got a sample card in the mail the other day, and I decided to give it a trial run. Here's how the session went:

I dialed the number printed on the card and listened while the friendly voice described how to punch in my six-digit meter number after the beep.

Having failed to determine my meter number, I punched in "111111".

The friendly voice asked me to verify that my street address was a particular four-digit number (that is now lost to memory) by pressing a particular key. It wasn't, of course, but I... ah... did. This is just a test run, right?

The friendly voice asked me to enter my meter reading. I punched in "1111".

The friendly voice thanked me for my cooperation and wished me a nice day.

Is it relevant that the rest of the day *was* relatively nice for me?

The upsides for The Company are quite apparent: the customer picks up the \$.06 cost of the call, while the Company saves both the postage and keypunch costs.

The Big Risk that was apparent to me in this system was that the friendly voice presented me with my street address and asked me to verify it, rather than the reverse. It's nice that they gave a bit of thought to verifying input, but isn't this approach a bit like presenting a computer user with the account password after the user name is typed and asking if it's correct? While it is true that there is no computer account to be hacked on the other side of this authentication mechanism (which is a strong malice motivator in the case of computer accounts), it is also true that there are hearts full of mischief in this world and big electric bills to be paid or protested if this system is implemented as proposed.

BTW, in the same mailing was a proposal for an alternate meter-reading scheme. The customer simply provides The Company with a copy of the key to the home, and the meter-reader simply lets self into the home to read the meter as necessary. Who can spot the risks in this one?

-Scott Rose

Stun belts -- who has the remote?

Jak Kirman <jak@cs.brown.edu> Thu, 14 Apr 94 00:10:31 +0100

AP and NBC reported recently on the use of REACT belts by police. Strapped around a prisoner's waist, the belts can deliver a 50,000-volt, 4-6 mA current to the prisoner's back muscles, enough to incapacitate the prisoner. They are activated by "a remote control like a garage-door opener". These belts are used on prisoners in transit and in court. The reports supplied no details concerning the communication between the remote device and the belt.

I wonder how much thought the designers gave to the possibility of unauthorized activation of the belt, e.g. by friends of the victim or simply out of malice. Judging by the footage on the NBC clip, it would be very hard indeed to get the belt off a prisoner who was being zapped by some unknown person.

If the remote device actively transmits start and stop commands, it might also be possible for an associate of the prisoner's to inhibit or curtail authorized activation; this would put the prisoner at a substantial advantage in an attempt at escape, since prisoners wearing the belt are not hand-cuffed, and are presumably not expected to make a run for it.

Can anyone supply technical details that would clarify the risks?

Jak Kirman jak@cs.brown.edu

Risks of Data Compression

Joe Decker <joe@synaptics.com> Mon, 11 Apr 94 11:06:05 PDT

An article in the most recent issue of _Weatherwise_ magazine contained a description of a system under development to send weather radar images to general aviation via data compression. One technique apparently used to minimize bandwidth was to not provide distinctions between the highest radar reflectivity levels, the idea being (according to the article) that you wouldn't want to be in a light plane in any of them. This neglects the RISK that you already are in one of them.

A more insidious RISK was not noted in the article. Many image compression methods result in images with misleadingly high amounts of detail. Such images could mislead pilots into making decisions based on false detail in the decompressed images. Image compression in safety-related applications clearly demands caution.

joe decker @synaptics.com @alumni.caltech.edu

TV Guide Contest

Agris Taurins <neodata!taurins@sterling.com> Tue, 19 Apr 1994 23:36:49 GMT

Is it just me, or has anyone else noticed the TNG contest in the April 23-29 issue of TV Guide?

As contests go, it's nothing terribly special. The winner(s) get flown out to Hollywood to watch the final episode. The most interesting item follows, directly out of the "Official Rules":

...To enter the sweepstakes electronically: Send your responses by April 29, 1994, to tvgtrek@delphi.com. Include name, address and telephone number, along with the answer to each of the seven questions. Sponsor not responsible for computer malfunctions; late, lost, or misdirected mail.

Earlier in the rules it states "Enter as often as you wish but limit one entry per envelope." The only "out" them might have is another line stating that "No mechanical reproductions will be accepted." But since they've explicitly stated that they're accepting electronic entries, I would think that it doesn't apply.

How many mailer daemons do you think will be spinning out there? How soon will it be (if it hasn't happened already) before the mail spool on delphi overflows?

Agris Taurins (402) 697-8006 taurins@neodata.uucpuunet!sparky!neodata!taurins

★ Re: MIT student arrest (Cohen, RISKS-15.76)

Dwight Silverman < Dwight. Silverman@chron.com> Mon, 18 Apr 94 21:52:54 CDT

Frederick B. Cohen, writing in the RISKS digest, muses about the case involving the MIT student arrested for having a BBS at that made commercial software available. Cohen implies that the student was unaware of the nature of the material at the site, an implication that I cannot let go unchallenged.

According to news reports about details in the indictment, the student not only was aware of what was being posted, but posted a public notice asking that the existence of the site not be trumpeted. The indictment, according to the reports, indicated he was more than just a "patsy."

Should MIT be "arrested," as Cohen suggested, because of the presence of this site on their machines? No, anymore than a phone company can be arrested because of telephone fraud. I've also seen comments on the Internet that those who uploaded the software should be arrested, as well. That's probably true, but it's not that easy. Again, according to news accounts, many of those who contributed to "Cynosure," as it was called, used anonymous account services to do so.

The RISK? Appear to be breaking the law, and you'll end up in a lot of trouble. It doesn't get much simpler than that.

Dwight Silverman, The Houston Chronicle dwight.silverman@chron.com

✓ Pointer to details on arrest of MIT student (Cohen, RISKS-15.76)

Sidney Markowitz <sidney@apple.com> Mon, 18 Apr 1994 19:14:07 -0700

[sidney markowitz <sidney@apple.com> SK8Board Punk Rocket Scientist Advanced Technology Group, Apple Computer, Cupertino, CA 95014]

Here is a pointer to information about the case of the MIT student who was

arrested recently. Although it is a solicitation for a legal defense fund, it contains presentations from both sides of the case and will be of interest to anyone who is interested in the broader political, moral and RISKy issues that are involved. In particular, this is not a simple case of software piracy or computer "hacking". The student is not being accused of copying copyrighted software, but only of operating a BBS that others used for that purpose. He is being charged under wire-fraud laws, being applied in a manner that is unusual, to say the least.

The following can be accessed via Mosaic or other World Wide Web client using the URL address

http://martigny.ai.mit.edu/dldf/home.html

Here's a quote extracted from the home page so you can see what is available there. In the actual Web version, the bulleted items at the end are hot links to their respective files.

The David LaMacchia Defense Fund was organized to ensure that David LaMacchia gets a fair trial. LaMacchia has been indicted by the federal government for conspiracy to commit wire fraud. "This is the first time in Massachusetts that the wire fraud statute has been used in a computer bulletin board case," said Stephen Heyman, deputy chief in the US attorney's office. That makes the case interesting, law-making, and very expensive. An unfortunate side-effect of our common law system, where laws are made by decisions in particular cases, is that an individual involved in a constitutional test case is faced with the certainty of staggering legal bills as well as the possibility of imprisonment and fines.

Contributions to the Fund will be used to defray a portion of LaMacchia's legal expenses. The Fund spends nothing on advertising, salaries, promotions, etc.; 100% of contributions are used for legal defense.

The Fund takes no position on the merits of either side's case.

Information from both sides

- * The Indictment
- * U.S. Attorney's April 7, 1994 press release
- * Response of Defense Counsel, April 8, 1994
- * Issues Primer (from Defense Counsel), April 11, 1994

Re: Green-Card Flap [Risks, Lawyers] (PGN, RISKS-15.76)

Ed Clarke <clarke@watson.ibm.com> Tue, 19 Apr 94 11:20:50 EDT

PGN omitted the quantity of mail that indirect.com received; 100 megabytes! They crashed of course as most systems would when presented with that kind of a mail overload. You also did not mention that this was the second time that they'd tried this trick (only about a hundred groups last time) and that they deliberately did not return the signed agreement that forbids this kind of abuse.

Posting their local phone number and FAX !!!! number was kind of cute though. Many more calls and faxes are going to the Tenn. Bar Association since that's where they are licensed.

By the way, you can add my (home) system to the "crashed" list. I get about 35 meg of compressed news per day, it jumped to 45 meg compressed and I ran out of inodes. Loss of news is similar to a crash. My down stream sites aren't going to see it, so it's loss of service anyway. The minor 5000 crossposts could be absorbed (at my site), but the huge amount of complaints in every bloody group killed me. Reminds me of the ping-pong ball demonstration of nuclear fission that was shown on TV when I was a kid. One ball gets tossed into a room full of ping-pong balls on mouse traps ... boom!

Ed Clarke clarke@acheron.UUCP clarke@watson.ibm.com

"Naissance d'un virus" by Ludwig/Condat

"Rob Slade, Ed. DECrypt & ComNet, 604-984-4067" <ROBERTS@decus.ca> Tue, 19 Apr 1994 10:06:47 -0600 (MDT)

BKNAISDV.RVW 940113

"Naissance d'un virus", Ludwig translated by Condat

I have previously reviewed Ludwig's original book (cf BKLUDWIG.RVW) and, basically, everything applies to this as well. I have only two brief comments to make on the translation.

I am rather surprised that a publishing house with the stature of Addison-Wesley took this on. I note that the promotional material which came with the book states that the original was banned for export from the United States. Even allowing for marketing hyperbole, they must have known that it would give rise to some kind of difficulties. As, indeed, it did: a recent court challenge has attempted to ban distribution of the book. I haven't yet heard the outcome. (I also note that the book is supposed to help you choose antiviral software: didn't they even read it first?)

The second addresses the issue of the educational value of the book. As previously noted, the text sections leave a great deal to be desired in terms of pedagogy. The viral code, however, is intact, and unchanged. All the comments are still in English.

(I am very amused to note that the French translation of "computer virus"--What? No, of course not. Don't be naive.--is CPA, standing for either "codes sources autopropageables" or "codes parasites autopropageables". This side of the pond CPA means a different sort of parasite.)

copyright Robert M. Slade, 1994 BKNAISDV.RVW 940113

Vancouver Institute for Research into User Security Canada V7K 2G6

Robert_Slade@sfu.ca rslade@cue.bc.ca p1@arkham.wimsey.bc.ca p1@CyberStore.ca

✓ IFIP SEC '94 Program [Excerpted from long message by PGN]

"Willis H. Ware" <Willis_Ware@rand.org> Fri, 08 Apr 94 11:29:46 PDT

The Tenth International Conference on Information Security - IFIP SEC'94

FOR FULL BROCHURE, CONTACT THE FOLLOWING:

FAX: IFIP SEC'94 SECRETARIAT +599 9652828

OR AIRMAIL TO: IFIP SEC'94 SECRETARIAT POSTOFFICE BOX 4 0 6 6 WILLEMSTAD - CURACAO NETHERLANDS ANTILLES CARIBBEAN

OR EMAIL TO: < TC11@IAIK.TU-GRAZ.AC.AT >

Organized by Technical Committee 11 of the International Federation for Information Processing, IFIP/TC 11 - in cooperation with the Special Interest Group on Information Security of the Dutch Computer Society - and hosted by the Caribbean Computer Society.

IFIP SEC'94

MAY 23-27,1994

ITC PISCADERA BAY

CURACAO, DUTCH CARIBBEAN

INTERNATIONAL PROGRAM

Dynamic Views on Information Security in Progress

***ABOUT THE TENTH INTERNATIONAL INFORMATION SECURITY CONFERENCE

This event is the Tenth in a series of conferences on information security. Something to celebrate. The organizers have compiled a truly exceptional, unique, and especially upgraded conference in a setting suitable for celebrating its Tenth birthday. Over 75 sessions will cover just about all aspects of information security, on a senior and advanced level. The formal language of SEC'94 is English. The proceedings are published by Elsevier North Holland in its acclaimed series.

INVITED PRESENTATIONS

Computer based cryptanalysis: man versus machine approach by Dr. N. Balasubramanian, former director of the Joint Cipher Bureau/ Cryptographic Services of the Department of Defense of the Government of India.

Establishing a CERT: Computer Emergency Response Team by Kenneth A. van Wyk, manager Assist team, Defense Information Security Agency of the Department of Defense, United States

Privacy aspects of data travelling along the new 'highway' by Wayne Madsen, scientist Computer Science Corp., United States

Issues in designing and implementing a practical enterprise security architecture by Ross Paul, manager information security, the Worldbank, United States

(key note's and other invited speakers to be announced by special bulletin)

IFIP TC 11 position paper in discussion: Security Evaluation Criteria by H. Schoone, Netherlands

Special TC 11 Working group sessions:

11.8 Computer Security Education, chair: Em. Prof. Dr. Harold Highland 11.1 IT Security Management, chair: Prof. S.H. von Solms (S. Africa)

11.5 System Integrity and Control, chair: William List (UK)

Special Appearance: Information Warfare: waging and winning conflict in cyberspace by Winn Schwartau (US)

Panel discussion: Panel discussion of the editors of Elseviers Journal Computers and Security chaired by John Meyer, Elsevier (UK), editor

Extended UNIX tutorial: Unix meets Novell Netware by Kevin H. Brady, Unix Systems Lab. (US)

Extended virus tutorial: Technologically enabled crime: shifting paradigms for the year 2000 by Sara Gordon (US)

Viruses: What can we really do? by Prof. Henry Wolfe (New Zealand)

Future trends in virus writing by Vesselin V. Bontchev (Bulgaria/Germany)

Viral Tidings by A. Padgett Peterson (US)

Integrity checking for anti viral purposes by Yisrael Radai (Israel)

Special appearance: *title to be announced* Prof. Eugene Spafford (US)

REFEREED PRESENTATIONS

Operations Security: the real solution to the problem - A. Don Temple (US)

Security in virtual reality: virtual security - Amund Hunstad (Sweden)

Prohibiting the exchange attack calls for hardware signature - Prof. Reinhard Posch/Wolfgang Mayerwieser (Austria)

Towards secure open systems - Dr. Paul Overbeek (Netherlands)

A security officer's workbench - Prof. Dennis Longley/Lam For Kwok (Australia/ Hong Kong)

An introduction to Citadel: a secure crypto coprocessor for workstations - Dr. Elaine Palmer (US)

On the calculation and its proof data for PI 10-9th - Shengli Cheng et al. (P.R. of China)

Securenet: a network oriented intelligent intrusion prevention and detection system - Ass. Prof. Dimitris Gritzalis et al. (Greece)

A methodology for the design of security plans - Drs. Fred de Koning (Netherlands)

An open architecture for security functions in workstations - Stefan Santesson (Sweden)

Security systems based on exponentiation primitives, TESS - Prof. Thomas Beth (Germany)

The structure and functioning of the COST privacy enhanced mail system - Prof. Sead Muftic, Nada Kapidzic, Alan Davidson (Sweden)

The need for a new approach to information security - Dr. Jean Hitchings (UK) A Practical database encryption system - Prof. C. Chang/Prof. D. Buehrer (Taiwan, ROC)

Security analysis and strategy of computer networks - Jie Feng et al. P.R.o.China)

Information Security: legal threats and opportunities - Dr. Ian Lloyd (Scotland)

Secure communication in LAN's using a hybrid encryption scheme - Prof. Mahmoud El-Hadidi, Dr. Nadia Hegazi, Heba Aslan (Egypt)

Secure Network Management - Bruno Studer (Switzerland)

Ramex: a prototype expert system for computer security risk analysis and management - Prof. Peter Jarratt, Muninder Kailay (UK)

The need for decentralization and privacy in mobile communications networks - D.I. Frank Stoll (Germany)

Is lack of quality software a password to information security problems ? - Dr. Peter Fillery, Nicholas Chantler (Western Australia)

Smart: Structured, multidimensional approach to risk taking for operational information systems - Ing. Paul van Dam, et al. (Netherlands)

IT Audit: the scope, relevance and the impact in developing countries - Dr. K. Subramanian (India)

Program structure for secure information flow - Dr. Jingsha He (US)

Security, authentication and policy management in open distributed systems - Ralf Hauser, Stefano Zatti (Switzerland/Italy)

A cost model for managing information security hazards - Love Ekenberg, Subhash Oberoi, Istvan Orci (Sweden)

Corporate computer crime management: a research perspective - Dr. James Backhouse (UK)

A high level security policy for health care establishments - Prof. Sokratis Katsikas, Ass. Prof. Dimitris Gritzalis, et al. (Greece)

Moss: a model for open system security - Prof. S.H. von Solms, Dr. P van Zyl, Dr. M. Olivier (South Africa)

The risk-based information system design paradigm - Dr. Sharon Fletcher (US) Evaluation of policies, state of the art and future research directions in database security - Dr. Guenther Pernul, Dr. A.M. Tjoa (Austria)

Exploring minimal ban logic proofs of authentication protocols - Anish Maturia, et al. (Australia)

Security concepts for corporate networks - Prof. Rolf Oppliger, Prof. Dieter Hogrefe (Switzerland)

The security process - Jeanette Ohlsson (Sweden)

On the security of lucas function - Dr. C.S. Laih (Taiwan RoC)

Security considerations of content and context based access controls - Donald Marks, Leonard Binns, Peter Sell, John Campbell (US)

Anonymous and verifiable databases: towards a practical solution - Prof. Jennifer Seberry, Dr. Yuliang Zheng, Thomas Hardjono (Australia)

A decentralized approach for authorization - Prof. Waltraud Gerhardt, Burkhard Lau (Netherlands)

Applying security criteria to a distributed database example - Dr. Marshall Abrams, Michael Joyce (US)

A comparison of international information security standards based on documentary microanalysis - Prof. William Caelli, Em. Prof. John Carroll (Australia/Canada)

Security in EDI between bank and its client - Pauli Vahtera, Heli Salmi (Finland)

Secure information exchange in organizations - D.I. Ralph Holbein (Switzerland) A framework for information system security management - Helen James, Patrick Forde (Australia)

The security of computer system management - Xia Ling et al. (P.R.o.China) Development of security policies - Jon Olnes (Norway)

Factors affecting the decision to report occurences of computer abuse - John Palmer (Western Australia)

Secure manageable remote access for network and mobile users in an open on-line transaction processing environment - Dr. James Clark (Singapore)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 78

Friday 22 April 1994

Contents

Computerized Traffic-Light Problems

Debora Weber-Wulff

Risks of winning

Stanley Chow

Computer Generates False Tsunami Warning in Japan

George Pajari

NYC subway fare cards double-deduct; UI at fault

Andrew Marc Greene

A consumer risk from Thomson Consumer Electronics

Re: we trust calculators over ourselves

John Powell

Re: Risks ... to the quality of science

A. Padgett Peterson

Re: Risks of Data Compression

John Kennedy

Re: Math and money laundering

Erann Gat

Peter Wayner

Re: Information resource

Edward Reid

Re: Green Card Posting

Caveh Jalali

Ned Kittlitz

Mark Brader

Info on RISKS (comp.risks)

Computerized Traffic-Light Problems

Prof_Weber-Wulff <weberwu@tfh-berlin.de> 20 Apr 1994 15:51:25 GMT

The Tagespiegel reports today (20 April 1994) on the new, computerized traffic light management system that the city installed at the large traffic circle

Ernst-Reuter-Platz. The 1.8 million mark (1.1 million \$) system went on line on Monday, and mastered the first wave of traffic well. After that, the traffic jams swelled to beyond normal proportions. Irate drivers complained by telephone and mail, but officials insisted that since it was now computer-controlled, it was okay. Apparently someone threatened legal action, and the city traffic board dispatched people with stopwatches to test the system. Sure enough, it was stuck in the early morning pattern, which was fine for handling inbound traffic, but disastrous in the afternoon rush hour. They have to go back to hand-switching the timing until they figure out what went wrong.

Debora Weber-Wulff, Professorin fuer Softwaretechnik und Programmiersprachen Technische Fachhochschule Berlin, Luxemburgerstr. 10, 13353 Berlin, Germany

Risks of winning

"stanley (s.t.h.) chow" <schow@bnr.ca> Wed, 20 Apr 1994 10:57:00 -0400

I just caught this on TV news last night:

A person won two consecutive keno games in the Montreal Casino. Since this is considered extremely unlikely, the police have been called in to investigate. The two games should have paid \$400K, but the winner has not yet been paid. He is instead doing the talk show circuit with how he analysed the numbers.

Supposedly, in the history of Nevada, the Keno jackpot has only been won once, which made his winning back to back somewhat unlikely. This happened on the electronic keno and has been shut down. The mechanic game is carrying on.

A one line comment by the reporter claimed that "a bug" in the computer repeated the sequence of number exactly every 4,000 games. This may be a case of someone picking a poor random number generator; but may well be the basis for police action. I understood that electronic slot machines are free running, merrily generating random numbers all day long, and pulling the lever merely selects the current number. This seems quite robust.

Stanley Chow InterNet: schow@BNR.CA (613) 763-2831
Bell Northern Research Ltd., PO Box 3511 Station C, Ottawa, Ontario
Me? Represent other people? Don't make them laugh so hard.

Computer Generates False Tsunami Warning in Japan

George Pajari <pajari@faximum.com> Wed, 20 Apr 94 10:55:17 PDT

RISKS readers will find this all too familiar...

>From the April 19th, 1994 edition of NHK's "Today's Japan", broadcast on KCTS (Seattle's PBS affiliate) 0100h PDT April 20th (as remembered):

Japan's weather bureau installed a new computer system for automatically generating tsunami warnings after earthquakes. The story implied that the machine was connected to various sensors around Japan and was configured to generate and communicate these warnings automatically.

During installation testing simulated data was input to verify the operation of the system. Unfortunately the machine had already been connected to the system that communicates tsunami warnings to the government and media and no one disconnected this communications link when the tests were run.

The predictable happened. The machine "detected" a potential tsunami, sent out the appropriate warning and at least two broadcast stations interrupted their normal programming to announce the impending tsunami. Obviously this caused some concern among the populace.

The problem was detected five minutes after the warning was first communicated but this was still sufficient time for the the warning to be broadcast.

pajari@Faximum.COM

George Pajari / Faximum Software / Tel: +1 (604) 925-3600 / Fax: ... 926-8182 1497 Marine Drive, Suite 300 / West Vancouver, BC / Canada V7T 1B8

NYC subway fare cards double-deduct; UI at fault

<Andrew_Marc_Greene@frankston.com>
Fri, 22 Apr 1994 09:10 -0400

[Source: The New York Times, 22 Apr 1994, p. B2]

The NYC subway has been introducing swipe cards which can be bought in five-ride increments. According to today's _Times_, citing an article in Thursday's _Newsday_, many riders are swiping improperly, causing a fare to be deducted from their card but not opening the turnstile. There's a display which instructs the rider to swipe again, but these are New Yorkers and have already decided to try another turnstile.

Apparently, the designers anticipated this problem and put in a solution -- if you swipe again at the same stile it doesn't deduct a second fare -- but didn't anticipate that harried/hurried Nyawkas wouldn't stop to read the display.

- Andrew Greene

A consumer risk from TCE

<[a source within TCE]>

Thu, 21 Apr 94 17:05:33 XXT

Thomson Consumer Electronics (TCE) is about to release a home entertainment product called the Digital Satellite Service (DSS) under the RCA brand. In short, this product is a small satellite dish (18" in diameter) that will allow customers to order video/audio programs from service providers. At this time the service providers are DirecTV (Hughes) and Hubbard (USSB). The system works as follows.

Upon purchase of a DSS system, the customer will receive a "smart-card" and then subscribe to one or more service providers. The customer can then view programs and order pay-per-view programs. The smart-card controls and tracks all purchases made with the DSS system. Information stored includes programs purchased, whether or not the programs were viewed, and the time the programs were viewed. This information is then transmitted (via telephone) to the service provider for billing purposes. The RISK? The service providers have the ability to build large databases of information on household viewing habits (e.g., John Smith views adult movies every Wednesday night between 10:00pm and 11:00pm). This information could then be sold to direct marketing firms, etc. There are laws that prevent cable companies from selling or releasing an individual's subscription information, but, to the best of my knowledge, the service providers for DSS are under no such obligation.

★ Re: we trust calculators over ourselves (Crawford, RISKS-15.76)

"John Powell" <p00929@psilink.com> Fri, 22 Apr 94 09:54:55 PDT

I had a similar situation last year when leaving a super expensive garage in downtown Chicago. The rates were 22.00 for 7-9 hours, and 40.00 for 9-24 hours. I had been there 8 hours and 50 minutes (I obviously was watching the clock closely with these stakes). When the attendant ran my timecard through the computer, it came up with \$40.00 as the rate.

The next 10 minutes I caused a significant backup as I refused to pay \$40 when the sign clearly stated the rate as 22. I got him to agree that the sign was right, and that I was there for less than 9 hours, but he still insisted that I owed him 40 ('cause the computer said so). I asked him to call a manager, he responded "I am the manager!!!!!". I spent the next several minutes describing to him the concept of rounding, and that the software obviously stunk and was written by thieves (or idiots or both). With these rates, the "thief" part was a given!

After a while he got the message that I was not going to pay more than 22, and decided to let his office figure it out later. After I paid him the \$22, I asked for a receipt. "I am sorry sir, but that is printed by the computer!!!". Another 2 minutes were spent figuring out how to write a manual receipt (which he had, but had never used!!).

John Powell <p00929@psilink.com>

★ Re: Risks ... to the quality of science (Tobis, RISKS-15.77)

A. Padgett Peterson, Information Security <padgett@tccslr.dnet.mmc.com> Wed, 20 Apr 94 08:14:59 -0400

>This issue was addressed in a remarkable essay by the eccentric and >curmudgeonly fluid dynamicist Clifford Truesdell. The essay is called "The >Computer: Ruin of Science and Threat to Mankind"

Something I have been noticing for some time is the loss of capabilities along certain lines of thought due to the dominance of others.

Actually the first evidence to me was when the hordes of Radio Shacks came out and all of the small shops disappeared. Suddenly it was difficult to find the "low volume" pieces amid the cheap plastic sound reproduction devices.

Later I became involved in a study of magnetic amplifiers and discovered that research in this country had essentially died out around 1957. I suspect that the rise of the transistor and integrated circuit which made no provision for the "L" in a "RLC" circuit. Young electronic engineers look at me strangely when I ask if they have heard of "Eli the ice man."

Think I'll hold onto my collection of steam engineering books 8*).

- > 5. Mathematics is the Science of Infinities. Computation is Essentially
- > Finite.

I suspect this is the real threat. In all of the cases mentioned above, dominance of the field has resulted in a reduction of the field as promising technologies are shunted aside for reasons other than technological. In the mid 1800s Samuel Colt might not have achieved prominence if it were not for the Czar's purchase of the entire output of Smith & Wesson for several years.

What if Motorola had not been inundated by orders for CPUs by General Motors in 1980 and the IBM-PC had been 68000 based with a 32 bit flat memory model? What if CPM/86 had been available (PC-DOS was actually choice four of three)? Should we "Think of it as Evolution in action" or "blind chance"?

Padgett

★ Re: Risks of Data Compression (Decker, RISKS-15.77)

John Kennedy <warlock@csuchico.edu> Thu, 21 Apr 1994 23:26:29 -0700

In a previous incarnation, I designed the graphical output of a weather radar system. As you can imagine, it was filled with concessions for the viewer's pleasure (mostly researchers, but some airports too).

At best, the output was lossy. Take a float, run it through an algorithm, convert it to a signed byte (+/- 127), and scrunch that down until you had about 16 possible different colors, many of which were set to the same value

(usually about 8 different colors total). Why? Storms were easy to spot, useful data crunching really couldn't be done with the eye because it was a slice through a cloud formation (particular in real-time PPI displays), etc. The expectations of researchers hadn't caught up with the physical & economic reality involved with the displays.

The end result was easy to use picture that could tell you where the wind was moving, usually involving about 8 different colors, often with lots of empty space (clear days were very boring). This data would compress quite well without data loss. I wouldn't have expected anyone to match high (towards) and low (away) velocity colors since they could mean a great deal to a pilot, especially in a small plane, but you certainly wouldn't like being in either situation.

The algorithms and noise present in the uncompressed data should warn anyone away from using the data too literally. You'd be surprised at the number of sites that planted a radar-blinding pole right by the dish, resulting in a large pie-shaped wedge taken out of every piece of data they ever generated.

John Kennedy <warlock@csuchico.edu>; Communications Services; USENET admin

✓ Math and money laundering (Wayner, RISKS-15.75)

Erann Gat <gat@aig.jpl.nasa.gov> Thu, 14 Apr 94 11:26:21 PDT

The following two articles appeared immediately following one another in RISKS 15.75:

>From: pcw@access.digex.net (Peter Wayner)
>Subject: God Grants Granite Gift to RISKS Punsters
>Subject: The Soft Pork Underbelly of Efficient Markets

The first article was about the inability of mathematical models to deal with the hairy edges of reality in the financial markets. The second article was about a way to use the futures markets to launder money in a way that was (the author claimed) essentially untraceable.

The irony of this juxtaposition is striking (so striking, in fact, that I am wondering if this is a coincidence or a masterful display of editorial subtlety) because the money-laundering scheme proposed by Peter Wayner won't work, despite the seemingly rock-solid mathematics that underlies it.

Wayner proposes to use the zero-sum property of the futures market to transfer money from A to B through the use of balanced trades. A and B respectively buy and sell an identical futures contract and then wait until market volatility has caused A to lose (and B to gain) the amount of money to be transferred, at which point A and B simultaneously get out of the market.

Some subtle clues leading to a reductio ad absurdum proof that this scheme is flawed can be found in the original text. For example, Wayner suggests that A and B use different brokers so that the coincidental trades will not be on the same set of books. So the scenario he proposes goes something like this: A

and B agree to a symmetric trade to be liquidated when the market reaches some predetermined price point, at which point money will have effectively transferred from A to B. After the initial agreement, there is no further communication between A and B. In fact, neither has any way of knowing whether or not the other party has in fact executed their side of the bargain, and it doesn't really matter. B's financial position depends only on the state of the market, which is not affected by whether or not A is playing (assuming the amounts of money involved are not extremely large).

In fact, B doesn't have to talk to A at all. There doesn't even have to be an A. B can just *pretend* that there is an A out there somewhere who has agreed to transfer money to B using Wayner's scheme, play the market, and make money. Or can he? The critical flaw in this scheme is in the following paragraph where Wayner describes (fleetingly) what happens when the market doesn't do what A and B expected it to:

>Person B sells the contract so that if the market goes down, i.e., the wrong
>way, then A and B together have lost no money. It's a zero sum. Now they just
>have to play the game a bit longer or for stakes that are twice as high. You

>can think of the process as flipping a coin until you have encounter a heads.

This little detail reveals this to be just another incarnation of a well known gambling system where bets are successively doubled on an even bet until you win. The problem with the scheme is that even a short run of losses requires a TREMENDOUS amount of capital to finance the exponentially increasing stakes required to stay in the game. In fact, you *can* make money using this scheme for a little while. The problem is that when you make money you don't make very much. When you eventually (and inevitably) encounter a long run of losses or unexpected market moves, you lose really big.

Laundering money through electronic markets works only if you can reliably predict the direction of the market. If you can do that, you don't have to launder money. On this particular RISK I think we can all rest easy.

Erann Gat gat@robotics.jpl.nasa.gov

Re: [gat@aig.jpl.nasa.gov (Erann Gat): Math and money laundering]

Peter Wayner <pcw@access.digex.net> Tue, 19 Apr 1994 22:59:28 -0400

Double or Doublecross? Your choice.

First, forget about thinking like a mathematician, a gambler or an upstanding citizen of Wall Street. You are some guy A who wants to move money to some guy B and you want to do it in as untraceable a way as possible. You're willing to pay extra for something that looks respectable and guys on Wall Street look real respectable in their braces and bespoke suits.

The old standbys, gold and gems, are fine, but they are hard to move safely. Plus you need an "explanation" for how you got them. Strange business

contracts are okay, but they demand some sort of front operation which takes time and money to run effectively.

So you turn to the futures market for the first try. Lets say you want to move n dollars. Luckily, both A and B have enough cash and borrowed funds on hand to sustain a loss of up to (2^i)n dollars. Let i=4 for the rest of this example, i.e. 16n dollars of loss reserves.

In 15 out 16 times, the progressive doubling system will work. The transaction will be close to untraceable. The only way that anyone would be able to prove that the transaction occurred would be if they could assemble both trading records and then match the trades. This can be shielded very effectively by trading in different countries with different exchanges and relying on arbitrageurs to keep the markets in line, but it tends to cost much more in transaction noise.

In 1 out of the 16 tries, things will go wrong. You might say they would go terribly wrong if you're a nervous criminal B who is afraid that A is going to doublecross him. Now A needs to get 16 n dollars fast. This is the big reason why A doesn't want to play the game alone or try and trick B into playing without A. If A mirrored the trades, the 16n dollars aren't in the pockets of a casino or the state lottery. They're just in A's pockets not B's. In reality, A and B are back where they were before futures markets were invented. They just need to move 16 times more money.

Your reaction to this depends upon the marginal cost of going back to the old fashioned money laundering tricks. I think at this point you just take a bigger truck to haul the gold. You do some trades with Van Goghs and Rembrandts instead of Cassats or Sisleys. In general, many of the transaction costs for security and other stuff are pretty fixed. Just remember that auction houses like Southeby's try to take 10% commissions, but they can be negotiated to be much lower for expensive works. Exciting record breaking prices attract attention and news.

The futures game is not perfect by any means. There _are_ transaction costs and problems in logistics. It works best if A+B can lock in exactly the same price on their trades. But when it is done, you can look at the world and say, "Gosh, I was completely at RISK! Thank God my Martingale scheme worked after all!" All the really smart mathematicians and sober IRS guys who never gamble because they know the odds will just accept it and think you're crazy to be doing this with your money. It comes with a built in insanity plea.

So, if your going to do this, choose i to suit your cash/RISKS profile. If you have more cash available, then you have a better chance of success. But hey, that's life.

★ Re: Information resource (RISKS-15.76)

Edward Reid <ed@titipu.resun.com> Wed, 20 Apr 94 11:08:33 EDT(-0400)

The message from Michael Enlow announcing an "information resource" is

junk mail which apparently has been broadcast widely on the Internet. My wife and I both received copies of this message. Neither of us has expressed any public interest in the topics Enlow mentions. Melynda attempted to reply to the email, asking why it had been sent to her unsolicited; in reply she received a listing of information from a mailer daemon. I wrote the "From:" address in the header asking the same question and have received no reply. I suspect that it was sent to RISKS by accident, simply by picking up the submission address in some dragnet for email addresses.

Enlow claims to be retired, but the listing sent by the "info" daemon lists two apparently active businesses. The info listing does not contain any advertising or solicitation. I have not retrieved any of the files listed, so I cannot comment on their value or on whether they contain advertising, except for one file which is clearly labeled as a catalog. The other files, from their titles, would appear to promote private investigation in general but not a specific business.

Enlow's information resource may valuable, but I object to his use of junk email to publicize that resource. That fact that he did not reply to my individual request makes me suspect his motives.

Edward Reid, PO Box 378, Greensboro FL ed@titipu.resun.com (normal)

Re: Green Card Posting

Caveh Jalali <Caveh.Jalali@eng.sun.com> Tue, 19 Apr 1994 21:31:55 +0800

[The 19 Apr 1994 New York Times Business Day section has a lengthy story entitled An Ad (Gasp!) in Cyberspace, by Peter H. Lewis, about the Green Card ad as its lead story. Here are some relevant details, via PGNed abstracting... For earlier details, see <u>RISKS-15.76</u> and 77. PGN]

Laurence A. Canter was quoted as saying, "We will definitely advertise on the Internet again. It appears to be a very profitable venture and a very viable vehicle for advertising a variety of things. I'm sure other businesses will be advertising on the network in the very near future."

Jeff Wheelhouse, system administrator for Internet Direct, Inc., was quoted as saying. "They will not be back on our system," He also said he would not be deterred by Mr. Canter's threat to sue Internet Direct for \$250,000 unless he is reconnected. "They crashed our computer about 15 times -- that's when we stopped counting -- because of the volume of incoming complaints," Mr. Wheelhouse said. "I lost an entire week dealing with this."

Wheelhouse said Internet Direct would remain firm, despite Canter's threat to sue Internet Direct for \$250,000 and restoration of their electronic mail privileges. That amount was what prompted Canter to say, "Conservatively, that's the amount of business we feel we will get out of this from the ad."

"The Internet is changing," Mr. Canter said. "People don't like the invasion

of what has been their private world. But as long as it's set up the way it is, where anyone has access to it, it's a public forum, and they have to accept anything that comes into it. "In fact," Mr. Canter added, "I've received a lot of calls from people who want to know how to do it." So pleased is he with the response, in fact, that he said he planned to write a book on how to advertise on the Internet.

[However, this suggests a grand strategy. Run an offensive ad, get chopped off, and then sue for the profits you did not make. PGN]

immigration posting overload and lawsuit

Ned Kittlitz <kittlitz@sw.stratus.com> Wed, 20 Apr 1994 12:28:47 -0400 (EDT)

[...] Rather than being wronged parties, it seems that C&S is flirting with a federal rap in the tradition of the Morris internet worm. An estimate of international expenditures of sysadmin time due to the C&S posting might be interesting.

E. N. Kittlitz (kittlitz@sw.stratus.com, kittlitz@world.std.com)

Speaking of green cards

<msb@sq.com> Wed, 20 Apr 1994 05:55:32 -0400

The most fun response to the Green Card Flap that I saw was in rec.games.bridge, where someone said "I don't understand why this was posted here; in this newsgroup we're only concerned with red and black cards"!

(There were followups, but you'd have to be into duplicate bridge to appreciate them.)



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 79

Tuesday 26 April 1994

Contents

Fax programming -- risk to politicians

Tom Keenan

Data Escape from Prison

Mich Kabay

Industrial espionage

Mich Kabay

Trojan @ U. Michigan

Mich Kabay

\$14 million QA failure

Mich Kabay

Security and Privacy panels

John Rushby

Strange Stalking

Flint Waters

UK Industrial Spy Law

Peter Sommer

Combination Locks I Have Known

Neil McKellar

Unusual Newspaper Error

Stewart Rowe

Risks of advertising on the net

Jerry Leichter

Updated addresses for Canter & Siegel

Paul Robinson

Re: MIT student arrested for BBS used ...

Tim Shepard

Douglas Rand

Re: NYC subway fare cards double-deduct

Mark Brader

Dan Lanciani

Padgett Peterson

Info on RISKS (comp.risks)

Fax programming -- risk to politicians

"Tom Keenan" <keenan@acs.ucalgary.ca> Mon, 25 Apr 94 18:40:56 MDT

According to the April 25/94 Globe and Mail:

Canadian Human Resources Minister Lloyd Axworthy is embarrassed by the leaking of a sensitive working paper to the press. It concerns government plans and "specifically indicated that Quebec wasn't going to get full control over job training any time soon." Unfortunately, an operator did not press the 0-2-1 fax code that would have sent it to English speaking provincial government offices. By hitting 1-2-1 instead, the working paper went to eight French language newspapers in Quebec, two of which eventually published stories on it.

Some are questioning whether it was indeed an error or the work of a saboteur. Reporters "marvel that a document of particular sensitivity to Quebec accidentally went to Quebec newspapers only."

Several years ago a similar faux pas occurred in the Canadian parliamentary press gallery when a young woman sent a detailed account of her romantic exploits of the past weekend by email to a female friend. She accidentally filed it with every newspaper's parliamentary reporter, but they were gentlemen and did not publish it.

Dr. Tom Keenan, I.S.P. Dean, Faculty of Continuing Education
University of Calgary 2500 University Dr. NW Calgary, AB T2N 1N4 CANADA
Voice: (403) 220-5429 FAX: (403) BUG-EXIT = 284-3948

Data Escape from Prison

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 26 Apr 94 12:13:52 EDT

>From the Associated Press newswire via Executive News Service (GO ENS) on CompuServe:

Inmates-Computers, By MARIA S. FISHER, Associated Press Writer

KANSAS CITY, Kan. (AP, 18 Apr 1994) -- The letter startled Nick Tomasic. It was from a prison inmate; other fellow prisoners, assigned to computerize records, had taken a Social Security number from an accident report and tried to sell it. Tomasic is the district attorney for Wyandotte County. It was his number.

The author makes the following key points:

- o 29 states and the federal government use prisoners for data entry.
- o The National Correctional Industries Association in Belle Mead, NJ scoffed at the potential risk of misuse, saying that in 12 years, there have been no cases of abuse.
- o Tomasic warned that criminals could determine addresses and phone

numbers of witnesses and victims during data entry.

- o In Johnson City, KS, Sheriff Kent P. Willnauer is looking into allegations that a prisoner passed Social Security numbers and other data to a confederate who opened fraudulent bank accounts.
- o Kansas State government officials insist that the data entry program saves taxpayers hundreds of thousands of dollars and that there is no danger to privacy or safety of residents.

Michel E. Kabay, Ph.D./ Dir. Education / Natl Computer Security Assoc.

Industrial espionage

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 26 Apr 94 12:13:39 EDT

>From the Reuter newswire via Executive News Service (GO ENS) on CompuServe:

CHINESE PAIR HELD IN TECHNOLOGY THEFT, By Robert Boczkiewicz

DENVER, April 15 (Reuter) - A federal judge cited national security concerns Friday when he refused to free a Chinese citizen who remains under house arrest charged with stealing software technology."

According to the author, the FBI arrested Wang Liaosheng and Jing Cui for an alleged theft of source code from Ellery Systems, Inc of Boulder, CO. Wang, a former employee of this firm, allegedly sold information to Beijing Machinery Import & Export (Group) Corp for \$550,000. The pair face charges of computer and wire fraud and could be punished by a maximum of 15 years in prison and \$500,000.

Michel E. Kabay, Ph.D./ Dir. Education / Natl Computer Security Assoc.

Trojan @ U. Michigan

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 26 Apr 94 12:13:46 EDT

>From the Washington Post newswire via Executive News Service (GO ENS) on CompuServe:

Message Posted On Internet Spurs Probe; Jokes, Threats Directed At African Americans

By John Burgess, Washington Post Staff Writer, 25 Apr 1994

The sordid side of the emerging electronic culture got a very public airing at the University of Michigan this month. Officials there are investigating an incident involving a stolen computer password and a death threat against African Americans that was sent over the global Internet

computer network.

The author continues with the following key points:

- o the perpetrator is still unknown.
- o On April 5, someone using a University of Michigan email address sent the offensive message to 30 newsgroups on the Net.
- o "Purporting to come from a group called the Organization for the Execution of Minorities, the posting was a lengthy collection of jokes and riddles directed against black Americans. It also contained rambling threats of death and injury."
- o The host system was immediately flooded with angry protests from around the Net.
- o The supposed originator protested his innocence and repudiated the message and its content.
- o Campus computer security specialists think the student may have been a victim of a classic Trojan Horse which collected logins and passwords by spoofing the login screen and writing the ID/password pairs to a file for retrieval.
- o International users also received the posting and criticized Americans for racism.

Michel E. Kabay, Ph.D./ Dir. Education / Natl Computer Security Assoc.

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 26 Apr 94 15:28:10 EDT

>From _The Globe and Mail_ [Canada], Mon 94.04.25 p. A3:

"Pensioners to keep overpayments: Ottawa to write off \$14 million mistake by computer."

According to the Canadian Press report, 8,000 pensioners received overpayments because the computer programs at the Canada Pension Plan did not correctly combine pensions. "...[I]t took years to uncover the mistake and figure out what to do about it."

[MK comments: what amuses me is the headline which blames the mistake on the computer. Quality Assurance, where art thou?]

Michel E. Kabay, Ph.D. / Dir. Education / Natl Computer Security Assoc.

Oakland posting for risks

John Rushby <RUSHBY@csl.sri.com> Sun 24 Apr 94 17:07:28-PDT

Last chance to register for

1994 IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY
May 16-18, 1994
Claremont Resort,
Oakland, California

The program for this, the main conference on computer security research, was posted in <u>RISKS-15.43</u>, 30 Jan 1994. I won't repeat the whole thing, but here are the details of the very exciting panels that have been arranged. These were missing from the earlier posting.

Monday 2:00--3:30 PANEL: Firewalls

Moderator: Steve Kent (BBN)

Panelists: Steve Bellovin (AT&T) -- "Firewalls are good"
Phil Karn (Qualcomm) -- "Firewalls are bad"

Tuesday 2:00--3:30 PANEL: What Security Needs To Learn From Other Fields

Moderator: Teresa Lunt

Panelists: Nancy Leveson (U. Washington) -- safety
Fred Schneider (Cornell) -- dependability
Jeffrey Voas (Reliable Software Technology) -- testing
Brian Snow (NSA) -- security perspective

There's still time to register. The easiest way to get the program and registration form is by WWW from http://www.csl.sri.com (follow the link under conferences), or by anonymous ftp of the file /pub/oakland94.txt from ftp.csl.sri.com. If all else fails, send email requesting the form to John Rushby (Rushby@csl.sri.com).

✓ Strange Stalking

Flint Waters <Flint.Waters@uwyo.edu> Tue, 26 Apr 1994 14:00:00 +0000 (M)

We just finished a pretty strange case.

A woman came in a reported that her estranged husband was stalking her. The officer that took the call started an investigation for the alleged stalking and contacted our County Attorney, (DA to most folks).

While investigating the matter the suspects lawyer turned over email from the wife to the husband soliciting contact. It started to look like a normal domestic situation where the complaint matches the mood.

Sgt Banks brought me the email so I could verify it and move on to other things. As I started looking into it things got strange. One of our campus systems is an Alpha running VMS and we have a special NEWUSER procedure which allows staff to create their own accounts, providing they know all of the important information about themselves.

As I investigated the accounts I found that the suspect and victims account were created within a few minutes of each other. I placed a trap on the logins to both accounts and soon learned that every access to her account was immediately preceded or followed by an access to his account and from the same computer.

Over the next several months I tracked the access to both accounts and watched as the suspect turned over more and more email from his wife. This guy was pretty creative in that he wrote long letters to himself and even changed his writing style to mimic hers.

We had a pretty solid interference case for the false evidence he was creating but it was only a misdemeanor. We really wanted to put together a felony due to some other crimes the suspect had committed, which were pending prosecution.

Finally, the wife decided to take a computer course on campus. The first day of class the students were told to create accounts on the campus computer system. Our victim went to the computer lab and followed all of the appropriate steps only to find she couldn't create an account because her authorization had been used already. Confused she went to her assigned User Consultant and complained that she was denied access.

The consultant, not knowing about my investigation, disusered the fraudulent account and helped the victim get a new one.

The gig was up since I was certain the suspect would realize we were watching him now. Fortunately, denial of computer service is a felony in Wyoming. We then pursued the arrest warrant. Several days later our suspect was arrested at his office on campus. When arrested he asked if he could call his attorney. When we said yes, he led us down the hall to a locked computer lab. He entered the code on the door and walked to the phone which sat two feet from the very computer that had been used to generate many of the fraudulant messages.

By now our case was pretty solid. The suspect was charged with Computer Crimes: Crimes Against Computer Users which carried a three year felony term, ten years if intent to commit fraud is proven.

Kinda heavy but pretty funny when you face the guy and he lies through his teeth. He thought he was dealing with a couple of Barney Fife's and he treated us like we were stupid. Obviously we didn't know what we were talking about and he had received all of the mail from his wife. We booked him and went back to work.

As it turned out, the joke was on us. On the day of the preliminary hearing the suspects lawyer arrived with a sworn affidavit from the wife. She decided that she had not been stalked and that her husband had not denied

her of any computer service. It appears a reconciliation is in the works.

Naturally we decided not to pursue prosecution with a hostile victim and our case was dropped. Really a shame considering the hours we had invested. The suspect has some federal time hanging over him on some other crimes but I really would have liked to see him lie on the stand about his computer feats.

Oh well. I never thought I'd have a computer-domestic disturbance.

UK Industrial Spy Law

Peter Sommer <hcorn@virtcity.demon.co.uk> Sat, 23 Apr 94 10:59:15 GMT

INDUSTRIAL SPY'S LEGAL LOOPHOLE TO BE CLOSED

Britain's industrial spies enjoy a legal loophole. If they access a computer to which they are not authorised, they can be found guilty under the Computer Misuse Act, 1990. If they manage to deceive an authorised user into giving them information from that computer, they almost certainly commit no offence. The UK government signaled on March 24th 1994 that it would introduce remedial legislation. However the precise form is still unclear and there appears to be no date for implementation.

English Law knows no concept of information theft - you can steal pieces of paper and data media containing information but there is no specific law protecting commercial secrets. The law is more concerned with catching the means of industrial espionage: bugging and tapping are criminal offences, respectively under the Wireless Telegraphy and Interception of Communications Acts. The Computer Misuse Act punishes unauthorised access without, in section 1, caring what the reason was.

Recent coverage by the BBC-TV's leading current affairs show Panorama and by the London Sunday Times has revealed that 200 UK pounds is the average rate charged by private detectives to assemble a dossier of an individual's bank balances, medical records and tax status. Nearly all of the information comes via abuse of this loop-hole. The technique is variously called the pretext call, the voice-hack, the imposter and the masquerade. The private detective assumes whatever "official" identity is necessary to mislead the bank clerk or government employee. Recently one "detective agency" has been circulating leading figures in the UK with offers to obtain critical data on any individuals in whom they were interested.

If any offence is being committed, it is probably by the computer owners, who, under the Data Protection Act, have an obligation to take appropriate steps to secure data under their control. (Eighth Principle, Data Protection Act, 1984). Data Protection obligations apply within the European Union.

A case in a magistrate's court (lowest level) last December suggested that there might be a way of extending the Computer Misuse Act to cover such third parties. Malcolm Farquharson induced a female employee of a cellular phone company to obtain details of cellular phone numbers and their ESNs (Electronic

Serial Numbers) so that he could fraudulently clone phones. The numbers were held on a computer to which the female employee had authorised access. Farquharson, but not the employee, was found guilty and sentenced to six months in prison although he had never touched the computer.

However legal experts believe that this case would not survive appeal to a higher court.

The UK Home Office say that the loophole will probably be closed by means of an amendment to the Data Protection Act but have so far produced no wordings nor a timetable. On April 10th, Home Secretary Michael Howard said that the Government was considering a new offence of gaining information by deception.

Even when the loophole is closed the abuse is likely to continue - enforcing a law where a telephone-based perpetrator is already doing a good job pretending to be someone else is never going to be easy.

Peter Sommer at the Virtual City London N4 4SR United Kingdom hcorn@cix.compulink.co.uk CompuServe: 100012,2610

Combination Locks I Have Known

Neil McKellar <mckellar@cs.ualberta.ca> Tue, 26 Apr 1994 13:56:55 -0600

I have owned four combination locks in my life. All of them were made by 'Dudley', a Canadian company. Admittedly, these are not top of the line locks. They were, however, the brand of lock officially "endorsed" by my school in grade 7 when I first got a locker. That was in 1979. I owned that lock until 1991 when it was broken into at the local gym. I immediately went out and bought the first 'Dudley' lock I picked out of a basketful in front of the local bookstore checkout counter. By mere coincidence, this lock had the same combination as my old one. I treated this as fortunate happenstance.

Later, I lost the new lock and was forced once again to replace it. Again, I selected the first lock in the basket. This time it had a different combination which I promptly forgot when the lock lay idle for six months. So this time, I purposely searched through the basket for a lock with MY combination on it. I found one in less than thirty seconds.

The locks are of the tumbler variety with markings from 0 to 59. I've tried my lock and I can be off by one marking when dialing the combination. Still, considering that I have successfully obtained 3 of 4 locks with the same combination, I'm tempted to go home tonight and try to "find" the combination I lost. Perhaps I'll even time myself.

Neil McKellar (mckellar@cs.ualberta.ca)

Unusual Newspaper Error

"Stewart Rowe" <usr2210a@tso.uc.edu> Fri, 22 Apr 1994 16:55:29 -0400

Perhaps one of your readers can explain how the Midwest edition of *The New York Times* today had a photo on the front page with the caption. "Joseph P. Kennedy Jr. being arrested at the White House yesterday", with no further explanation or story anywhere in the paper?

Stewart Rowe usr2210a@tso.uc.edu

Risks of advertising on the net

Jerry Leichter <leichter@Irw.com> Tue, 26 Apr 94 08:23:08 EDT

In their Internet advertising, Canter and Siegal are ignoring some fundamental characteristics of the net as currently constituted. I think they'll find their attempt at Internet advertising will fairly quickly become ineffective - though many people may be annoyed along the way.

The relevant characteristics of the Internet are (a) the anonymity; (b) the low cost of generating any particular kind of message. What, after all, prevents anyone from taking a C&S ad, modifying it slightly - changing the addresses and phone numbers, for example - and posting it back as widely as the original? If only a few people do this, it will be impossible to tell which are the real ads and which are fakes - short of calling a phone number and finding that it terminates, say, at the Bar Association rather than C&S.

Of course, ads that mention price will raise even more severe problems. If the spoof suggests a completely unreasonable price, the business can probably disclaim it. But what happens when the spoof suggests a reasonable-looking price that happens to leave the advertiser with no profit? He is left the the choice of accepting the price, and losing money, or disclaiming the ads, damaging his own reputation.

Traditional printed ads can, of course, also be spoofed. However, attempts to do so are rare. First, it's very expensive to do; second, the traditional at least attempt to verify the identity of advertisers. Neither of these constraints apply on the net.

It's true that a careful reading of the header lines will often reveal which are the true ads, and which are the fakes. But why should the people who the ad is trying to reach bother to check header lines? The whole point of an ad is to communicate information quickly. The same reasoning shows that digital signatures wouldn't help. Who would bother to check them? Only those who have an established relationship with the sender of the ad would likely even have a quick ability to verify the signature - and that's not the population a broadly distributed ad is trying to reach.

When the spoofers are traceable - and it's well known that it's often impossible to trace a message, much less *prove* that a particular individual sent it - the legal situation might get rather interesting. Even ignoring the

very broad protection the courts have recently granted to parody, why is the spoofer's message any less legitimate than the original? If the spoof ads look entirely different, refer to "Carver and Siegalman", and have different addresses and phone numbers, just what right to "Canter and Siegal" have to complain? They are not being directly referred to or identified. If they have a problem establishing a unique identity in the noise of the marketplace - and no one ever said that all marketplace participants have to be genuine - that's not the law's concern.

-- Jerry

✓ Updated addresses for Canter & Siegel

Paul Robinson <PAUL@TDR.COM> Fri, 22 Apr 1994 14:24:08 -0400 (EDT)

This list should help in setting up kill files or to watch for later posts:

Sender: LISTSERV list owners' forum <LSTOWN-L@SEARN.BITNET>

Poster: Wes Morgan <morgan@ENGR.UKY.EDU>

Subject: Updated addresses for Canter & Siegel [mispeling curekted]

It appears that Canter & Siegel, the law firm which recently flooded both Usenet and LISTSERVs with their "Green Card Lottery" posting, have secured access to the net through many sources. For those of you interested in blocking their access to your list, here is the current collection of addresses for that firm.

cslaw@delphi.com

cslaw@win.net

cslaw@witchcraft.com

cslaw@pipeline.com

cslaw@netcom.com

cslaw@indirect.com (currently disabled)

lcanter@delphi.com

lcanter@win.net

lcanter@witchcraft.com

lcanter@pipeline.com

Icanter@indirect.com (currently disabled)

76636.443@compuserve.com

They also, apparently, have sites of their own; those sites are lcanter.win.net and msiegel.win.net.

In an article in Tuesday's _New York Times_, Mr. Carter basically said, "this was immensely profitable; we will be doing this in the future." Forewarned is forearmed...

--Wes

★ Re: MIT student arrested for BBS used ... (Cohen, RISKS-15.76)

Tim Shepard <shep@lcs.mit.edu> Wed, 20 Apr 94 15:47:49 -0400

I've been closely following the accounts of this case in the Boston Globe and The Tech (a student-published newspaper at MIT). Until your report, I had not heard any assertions that the student had actually been arrested.

According to an article in The Tech on Friday April 8th, 1994:

"A federal grand jury charged an MIT student yesterday on a felony charge for allegedly allowing the piracy of over \$1 million in business and entertainment software using Athena workstations."

According to an article in The Tech on Tuesday April 12th, 1994:

"David M. LaMacchia '95, who was indicted last Thursday for conspiracy to commit wire fraud, will be arraigned this Friday at the U.S. District Courthouse in Boston, according to LaMacchia's lawyer Harvey Silverglate."

Other than Cohen's article, and a couple of followup articles in RISKS DIGEST, I've seen no report that he had been actually arrested. I cannot imagine why he would need to be arrested. (I would expect that if he already has a lawyer, and the lawyer knows of the scheduled arraignment three or more days beforehand, he would most likely show up in court. Maybe I missed something. What was your source?)

-Tim Shepard

★ Re: MIT student arrested for BBS used ... (Cohen, RISKS-15.76)

Douglas Rand <drand@osf.org> 25 Apr 94 17:50:35

In his post, Fredrick Cohen states "An MIT student was arrested today for having a BBS at the school that was used by the participants to store and fetch commercial software." and goes on to paint the student as practically an innocent bystander caught up in other peoples crimes by happenstance. If one is to believe any of the reportage on the real incident, the student was anything but innocent.

All the reportage in the Boston Globe, not known for its great sympathy with law enforcement, made it quite clear that the student actively advertised his BBS as a place to upload and download pirated software. He went out of his way to personally solicit software on at least some occasions (according to the reports).

In this, he would be guilty of various crimes regardless of the means he used to carry the crimes out. While I feel a little sorry for him, in that he probably felt he was carrying on some idealistic fight, I don't feel particularly sorry for him, and he deserves to be prosecuted.

Let's save our righteous indignation for the truly innocent, wrongly accused and persecuted by people in power.

Doug Rand <drand@osf.org> Open Software Foundation, Motif Development

Re: NYC subway fare cards double-deduct (Greene, Risks-15.78)

Mark Brader <msb@sq.sq.com> Mon, 25 Apr 1994 18:57:58 -0400

Okay, so how exactly is it possible in this system for the turnstile to (a) deduct the fare from the card, and (b) identify whose card it was, so that it won't deduct it again if the same card is re-swiped -- and yet not figure out that it now has to unlock itself?

By the way, what happens if the turnstile does unlock, and the rider hands the card back across the barrier to someone else? Will the second rider get admitted without a second fare being deducted, because the same card was used?

Mark Brader, msb@sq.com SoftQuad Inc., Toronto

[Also related comments from dan@wais.com (Dan Aronson) and sullivan@geom.umn.edu (John Sullivan). PGN]

Re: NYC subway fare cards double-deduct; UI at fault (Greene)

Dan Lanciani <ddl@das.harvard.edu> Fri, 22 Apr 94 17:53:16 EDT

I can't let this pass without comment. Clearly this system was designed by someone obsessed with the RISKs of free rides. The only way I can imagine this kind of failure mode occurring is if they are doing something along the lines of <read>

✓ Double your pleasure in the subway (Greene, RISKS 15.78)

Fri, 22 Apr 94 14:08:39 -0400

Wonder if they put a limit on the "swipe again" - sounds like a new kind of "family plan".

Padgett



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 80

Thursday 28 April 1994

Contents

DMV Computer upgrade goes awry...

Marshall Clow

Time-series wins jackpot

Mich Kabay

Drunk in charge.....

Kearton Rees

Stress Analysis of a Software Project [long]

Jerry Leichter

Info on RISKS (comp.risks)

DMV Computer upgrade goes awry...

Marshall Clow <mclow@coyote.csusm.edu> Wed, 27 Apr 1994 11:03:47 -0700

DMV careens into \$44 million dead-end By Gary Webb, Knight-Ridder News Service (From the San Diego Union, April 27, 1994, page A-3)

SACRAMENTO - The California Department of Motor Vehicles has informed a flabbergasted legislative committee that it has spent \$44.3 million on a computer modernization program that will never work.

"This is unconscionable to me!" Assemblywoman Valerie Brown, D_Santa Rosa spluttered. "I can't even explain this to people!"

DMV Director Frank Zolin muttered: "I'm having a difficult time explaining it myself." [...]

"The department's position is that the software maker isn't responsible, the hardware maker isn't responsible, and the taxpayers are just going to eat the cost", Transportation Committee Chairman Richard Katz, D-Panorama Ciry, said after the Monday hearing. [...]

The DMV started the project in 1988 and has been quietly spending millions of dollars a year on it with little oversight - and even less success. ... Dan Foulk, a Sacramento computer consultant who has been working with the DMV on the ill-fated venture, called it "a combination of errors from the

beginning". Faulk said that the plan - to invisibly convert a circa-1965 database to a modern relational database using Tandem Cyclone mainframes - was "too giant a leap of technology" and involved insurmountable incompatibilities beween hardware platforms and program code. [...]

The \$7.5 million the DMV was requesting in next year's budget was to be used to start redesigning the database from scratch, records show. But Zolin said that it is "not exactly" a back-to-square-one proposition.

"We've learned a lot from mistakes we made", he said.

===========

(Excerpt from the San Jose Mercury News, April 27, 1994 online version:) Ernst & Young, an accounting and consulting firm hired to oversee the five-year project, was fired by the state in June 1990 after just eight months on the job. DMV then took on the task of project management itself -- a herculean undertaking that legislative analysts now say was well beyond the department's ability. ...

We've all seen this before, this is just larger and more public than many.

Marshall Clow, mclow@san_marcos.csusm.edu

Time-series wins jackpot

"Mich Kabay / JINBU Corp." <75300.3232@CompuServe.COM> 28 Apr 94 14:40:25 EDT

"Casino finally pays big keno winners: Montreal computer analyst hopes \$620,000 jackpot will give others hope. By Andre Picard, Quebec Bureau. The _Globe and Mail_ (Canada), 28 Apr 1994, p. A6 [MK comments in brackets]

Montreal -- Daniel Corriveau said he hopes that his 'victory over the system will give hope to others.'

The computer analyst and his family received more than 620,000 [1C\$ = U\$0.75], including interest, from the Montreal casino yesterday, weeks after they overcame odds of one in six billion and beat an electronic keno game three times in a row."

The author explains the following key points:

- o Corriveau used an "antique 286" computer to analyse 7,000 combinations from the keno game, [which uses an electronic pseudo-random number generator].
- o Corriveau noticed that the electronic game was repeating numbers in a predictable pattern.
- o Corriveau and several family members bet on what they predicted would be due to come up; they won three times in succession.
- o The Casino managers shut the game down and called the police.
- o The Surete du Quebec [provincial police] fraud squad investigated; Corriveau

and his family even took polygraph tests.

- o The president of Loto-Quebec, the Crown Corporation which owns the Montreal Casino, admitted that the problem was theirs: they had failed to test the electronic game before using it.
- o The keno game is missing its clock, [used to reset the pseudo-random number generator]; therefore it started all over again every time it was powered off.
- o Police are continuing their investigation to find out if the clock was missing when the game was delivered or whether it has been stolen.

[Sigh... quality assurance rears its missing head once again. And bravo for the successful time-series analyst. Wonder if he'd like to have a go at the Clipper Chip?]

Michel E. Kabay, Ph.D. / Dir. Education / Natl Computer Security Assoc.

drunk in charge.....

<krees@minster.york.ac.uk>
Wed, 27 Apr 94 13:32:25

I am a member of a mailing list covering motorcycling and related topics.

Recently much discussion revolved around the issue of drinking (alcohol) and driving, and what, if any, the limit of alcohol allowed in the blood should be. Discussion seemed to revolve around the point that the effect that alcohol has varies with a number of individual factors.

One comment however I think is of interest to this forum.

The comment was made that alcohol in whatever quantity, affects your ability to judge whether you are fit to perform an act such as driving. The example used to illustrate this was that electricians never touch any of their work that might involve high-voltage electricity after they have been drinking, because of the possible consequences.

Extending this argument to computing. How many people would be happy flying in a plane, or placing their trust in a software controlled system if they knew that it had been written, reviewed or tested after a Friday lunchtime in a pub. To the electrician the possible are obvious and immediate. To programmers etc. the consequences may be neither obvious nor immediate.

Should there be an offence of "drunk in charge of a computer"? Probably not. But I think that this sort of issue be addressed, and any legal implications considered, possibly in professional codes of conduct?

Kearton Rees, High Integrity Systems Eng. Group, Computer Science Dept., University of York, Heslington Road, York, YO1 5DD. krees@cs.york.ac.uk Tel.: 0904-433385

Stress Analysis of a Software Project [long]

Jerry Leichter <leichter@lrw.com> Tue, 26 Apr 94 08:42:32 EDT

The following, which claims to be an internal Silicon Graphics memo, has already seen fairly broad network distribution. I have no way of verifying that it is what it claims to be, but (a) I'm told by someone with close dealings with SGI that it fits with what he's heard; (b) if it's a fake, someone put a huge amount of effort into producing it.

I forward it to RISKS as a wonderful record of what goes wrong with large software projects, and why. It would be as useful if all the names, including the company and product names, were removed. This memo should not be seen as an indictment of SGI, which is hardly unique. There is good evidence that Sun, for example, had very similar problems in producing Solaris; and I watched the same thing happen with the late, unlamented DEC Professional series of PC's, and something like it almost happen with firmware for DEC terminals a number of years back.

I hope that Tom Davis's position hasn't been badly hurt by the broad distribution of his memo - but based on the traditional reaction to bearers of bad news, especially when the bad news becomes widely known, I can't say I'm sanguine about it.

-- Jerry

----- Begin Document -----

Software Usability II October 5, 1993 Tom Davis

Last May, I published my first report on software usability, which Rocky Rhodes and I presented to at Tom Jermoluk's staff meeting (with Ed, but without Tom). Subsequently, I made it available to quite a few other people.

This sequel is to satisfy all those people who have urged me to bring it up to date. I begin with a summary; details follow.

Please read at least the summary.

SUMMARY

Release 5.1 is a disappointment. Performance for common operations has dropped 40% from 4.0.5, we shipped with 500 priority 1 and 2 bugs, and a base Indy is much more sluggish than a Macintosh. Disk space requirements have increased dramatically.

The primary cause is that we attempted far too much in too little time. Management would not cut features early, so we were forced to

make massive cuts in the final weeks of the release.

What shall we do now? Let's not look for scapegoats, but learn from our mistakes and do better next time.

A December release of 5.1.2 is too early to fix much -- we'll spend much more time on the release process than fixing things. Allow enough time for a solid release so we don't get: 5.1.2.1, 5.1.2.2, 5.1.2.3, ...

Let's decide ahead of time exactly what features are in 5.1.2. If we pick a reasonable set we'll avoid emergency feature cuts at the end.

Nobody knows what's wrong -- opinions are as common as senior engineers. The software environment is so convoluted that at times it seems to rival the US economy for complexity and unpredictability. I propose massive code walk-throughs and design reviews to analyze the software. We'll be forced to look closely at the code, and fresh reviewers can provide fresh insights.

For the long term, let's change the way we do things so that the contents and scheduling of releases are better planned and executed. Make sure marketing and engineering expectations are in agreement.

INTRODUCTION

We've addressed some of the problems presented in the original May report, but not enough. Most of the report's warnings and predictions have come true in 5.1. If we keep doing the exact same thing, we'll keep getting the exact same results.

I'm preparing this report in ASCII to make it widely available. It's easy to distribute via news and mail, and everyone can read it.

An ASCII version of the May 12 report can be found in:

bedlam.asd:/usr/tmp/report.text

The included quotations are not verbatim. Although the wordings are inexact, I believe they capture the spirit of the originals.

BLOAT UPDATE

"Do you want to be a bloat detective? It's easy; just pick any executable. There! You found some!"

-- Rolf van Widenfelt

In the May report, I listed a bunch of executable sizes, and pointed out that they were unacceptable if we intended to run without serious paging problems on a 16 megabyte system. Between May and the 5.1 release, many have grown even larger. IRIX went up from 4.8 megabytes to 8.1 megabytes, and has a memory leak that causes it to grow. Within a week, my newly-booted 5.1 IRIX was larger than 13.8 megabytes -- a big chunk of a 16 megabyte system. It's wrong to require our users to

reboot every week.

There are too many daemons. In a vanilla 5.1 installation with Toto, there are 37 background processes.

DSOs were supposed to reduce physical memory usage, but have had just the opposite effect, and their indirection has reduced performance.

Programs like Roger Chickering's "Bloatview" based on Wiltse Carpenter's work make some problems obvious. The news reader "xrn", starts out small, but leaks memory so badly that within a week or so it grows to 9 or 10 megabytes, along with plenty of other large programs. But what's really embarrassing is that even the kernel leaks memory that can't be recovered except by rebooting!

Showcase grew from 3.2 megabytes to 4.0 megabytes, and the master and status gizmos which are run by default occupy another 1.7 megabytes. Much of this happened simply by recompiling under 5.1 -- not because of additional code.

The window system (Xsgi + 4Dwm) is up from 3.2 MB to 3.6 MB, and the miscellaneous stuff has grown as well. As I type now, I have the default non-toto environment plus a single shell and a single text editor, jot. The total physical memory usage is 21.9 megabytes, and only because I rebooted IRIX yesterday evening to reduce the kernel size. Luckily, I'm on a 32 megabyte system without Toto, or I'd be swamped by paging.

Much of the problem seems to be due to DSOs that load whole libraries instead of individual routines. Many SGI applications link with 20 or so large DSOs, virtually guaranteeing enormous executables.

In spite of the DSOs, large chunks of Motif programs remain unshared, and duplicated in all Motif applications.

PERFORMANCE UPDATE

"Indy: an Indigo without the 'go'".

-- Mark Hughes (?)

"X and Motif are the reasons that UNIX deserves to die."

-- Larry Kaplan

The performance story is just as bad. I was tempted to write simply, "Try to do some real work on a 16 megabyte Indy. Case closed.", but I'll include some details.

In May, I listed some unacceptable Motif performance measurements. Just before 5.1 MR, someone reran my tests and discovered that the performance had gotten even worse. Some effort was expended to tune the software so that instead of being intolerable, it was back to

merely unacceptable performance.

We no longer report benchmark results on our standard system. The benchmarks are not done with the DSO libraries; they are all compiled non-DSO so that the performance in 5.1 has not declined too much.

Before I upgraded from 4.0.5 to the MR version of 5.1, I ran some timings of some everyday activities to see what would happen. These timings were all made with the wall clock, so they represent precisely what our users will see. I run a 32 megabyte R4000 Elan.

Test	4.0.5	5.1	% cł	nange	
		-			
C compile		25 sec	35 s	ec 40%	
C++ comp small app		68 sec	105	5 sec 54%	6
Showcase startup, 13 sec May report file			18	18 sec 38%	
Start a sh	ell <2	sec	~3 sec	~50%	
Jot 2 MB	file <2	2 sec	~3 sec	~50%	

What's most frightening about the 5.1 performance is that nobody knows exactly where it went. If you start asking around, you get plenty of finger-pointing and theories, but few facts. In the May report, I proposed a "5% theory", which states that each little thing we add (Motif, internationalization, drag-and-drop, DSOs, multiple fonts, and so on) costs roughly 5% of the machine. After 15 or 20 of these, most of the performance is gone.

Bloating by itself causes problems. There's heavy paging, there's so much code and it's so scattered that the cache may as well not be there. The window manager and X and Toto are so tangled that many minor operations like moving the mouse or deleting a file wake up all the processes on the machine, causing additional paging, and perhaps graphics context swaps.

But bloat isn't the whole story. Rocky Rhodes recently ran a small application on an Indy, and noticed that when he held the mouse button down and slid it back and forth across the menu bar, the (small) pop-up menus got as much as 25 seconds behind. He submitted a bug, which was dismissed as paging due to lack of memory. But Rocky was running with 160 megabytes of memory, so there was no paging. The problem turned out to be Motif code modified for the SGI look that is even more sluggish than regular Motif. Perhaps the problem is simply due to the huge number of context swaps necessary for all the daemons we're shipping.

The complexity of our system software has surpassed the ability of

average SGI programmers to understand it. And perhaps not just average programmers. Get a room full of 10 of our best software people, and you'll get 10 different opinions of what's causing the lousy performance and bloat. What's wrong is that the software has simply become too complicated for anyone to understand.

WHAT WENT WRONG IN 5.1?

The one sentence answer is: we bit off more than we could chew. As a company, we still don't understand how difficult software is.

We planned to make major changes in everything -- a new operating system, new compilers, a new user environment, new tools, and lots of new features in the multi-media area. Not only that, but the new stuff was promised to do everything the old software had done, and with major enhancements. (Early warning: version 6.0 promises to be even more disruptive.)

About 9 months ago, Rocky and I pointed out the impossibility of what we were attempting. Rather than reduce the scope of the projects, a decision was made to hire a couple of contractors (who know nothing about our system) to handle the worst user interface problems in the Roxy project. In addition, promises were obtained from various executives that a significant effort would be made to improve software performance.

Management was basically afraid to cut any features, so we continued to work on a project that was far too large. The desperate attempt to do everything caused programmers to cut corners, with disastrous effects on the bug count. And the bug count was high simply because 5.1 was so big.

Only when the situation was beyond hope of repair did we start to do something. Features and entire products were removed wholesale from the

release, and hundreds of high-priority bugs were classified as exceptions, so that we could ship with "no priority 1 and 2 bugs". We did, however, ship with over 500 "exceptions". The release was deemed too crummy to push to all our machines, but was restricted to the Indys, the high-end machines, and a few others where new hardware required the new software. Due to the massive bug count, virtually no performance tuning was done.

When the schedule is impossible as it was in 5.1, the release process itself can get in the way. The schedule imposes a code freeze long before the software is stable, and fixing things becomes much more difficult. If you know you're going to be late, slip before the code freeze, not after. We're trying to wrap up the box before the stuff inside is finished, and then trying to fix things inside the box without undoing the wrapping -- it has to be less efficient.

Management Issues:

There was never an overall software architect, and there still is not, and until Way Ting was given the job near the end, there was no manager in charge of the 5.1 release, either.

I wrote a note in sgi.bad-attitude about the "optimist effect", which I believe is mostly true. In condensed form:

Optimists tend to be promoted, so the higher up in the organization you are, the more optimistic you tend to be. If one manager says "I can do that in 4 months", and another only promises it in 6 months, the 4 month guy gets the job. When the software is 4 months

late, the overall system complexity makes it easy to assign blame elsewhere, so there's no way to judge mis-management when it's time for promotions.

To look good to their boss, most people tend to put a positive spin on their reports. With many levels of management and increasing optimism all the way up, the information reaching the VPs is very filtered, and always filtered positively.

The problem is that the highly filtered estimates are completely out of line with reality (at least in recent software plans here at SGI), and there are no reality checks back from the VPs to the engineers on the bottom. I think it's great to have aggressive schedules where you try to get things out 20% or so faster than you'd expect. The problem is that in 5.1, the engineers were expected to get things out 80% faster, and it was clearly impossible, so many just gave up.

We certainly didn't win any morale prizes among the engineers with 5.1. It's the first release here at SGI where most of the engineers I talked to are ashamed of the product. There are always a few, but this time there were many. When engineers were asked to come in over the weekends before the 5.1 release to fix show-stopper bugs, I heard a comment like: "Why bother? SGI's going to release it anyway, whether they're fixed or not."

I'm not blaming the engineers. Most of them worked their hearts out for 5.1, and did the best they could, given the circumstances. They'll be happy to buy into a plan where there's a 20% stretch, but not where there's an 80% stretch. They figure: "It's hopeless, and I'll be late anyway, and I'm not going to get rewarded for that, so why kill myself?"

Marketing - Engineering Disconnect

"Marketing -- where the rubber meets the sky."

-- Unknown

There's a disconnect between engineering and marketing. It's not surprising -- marketing wants all the whiz-bang features, it wants to run in 16 megabytes, and it wants it yesterday. Although engineering would like the same things, it is faced with the reality of time

limits, fixed costs, and the laws of nature.

It's great to have pressure from marketing to do a better job, but at SGI, we often seem to have deadlocks that are simply not resolved. Marketing insists that Indy will work in 16 megabytes and engineering insists that it won't, but both continue to make their plans without resolving the conflict, so today we're shipping virtually useless 16 MB systems. Similarly for feature lists, reliability requirements, and deadlines.

Well, at least we met the deadline.

WHAT TO DO -- SHORT TERM (5.1.2)

"We should sell 'bloat credits', the way the government sells pollution credits. Everybody's assigned a certain amount of bloat, and if they go over, they have to purchase bloat credits from some other group that's been more careful."

-- Bent Hagemark

There are problems in both performance and bugs, and we'd like to fix both. In addition, the first thing we should do is decide exactly what's going into release 5.1.2.

If we are serious about a December all-platforms release, there may be very little we can do other than keep stumbling along as we have been. Three months isn't much time to do anything, considering the overhead of a release, where perhaps half of the time will be spent in "code freeze". After 5.1, many engineers are exhausted, and it's unreasonable to expect them to start hard work immediately. 500 outstanding priority 1 and 2 bugs is a huge list, and we haven't even begun to hear about customer problems yet.

What Should be in Release 5.1.2:

I'm afraid the answer is going to be "everything that didn't make it into 5.1". I know that won't be the case, but I hope that we will carefully select what goes in now, rather than hack things out in a panic in December. The default should be "not included", and we should require a good reason to include things. Let's make sure that there's a minimal, solid, working set before we start adding frills.

Improving Performance:

"SGI software has a cracked engine block, and we're trying to fix it with a tune-up."

-- Mark Segal

As stated above, we don't even know exactly what's wrong. We probably never will, but we should start doing things that will have as much of

an impact on the problem as possible. I don't think we have time to study the problem in detail and then decide what to do -- we've got to mix the research with doing something about it.

Before we begin, we should have definite performance goals -- lose less than 5% wall-clock time on compiles of some known program over 4.0.5, have shells come up as fast as in 4.0.5, or whatever.

Some people claim that we need new software debugging tools to look at the problem, and that may be true, but it's not a short-term solution, and it runs the risk of causing us to spend all our time designing performance measurement tools, rather than fixing performance.

In fact, I don't really believe that simple "tuning" will make a large dent. To get things to run significantly faster, we've got to make significant changes. And we can't beat the "5% rule" by just speeding up all the systems by 5% -- if everything is exactly 5% faster.

the overall system will be exactly 5% faster.

There's a strong tendency to look for the "quick fix". "Get the code re-arranger to work", or "Put all the non-modifiable strings in shared code space", for example. These ideas are attractive, since they promise to speed up all the code, and they should probably be pursued, but I think we're not going to make a lot of progress until we identify the major software architectural problems and do some massive simplification. Remember that DSOs were the last "quick fix".

There's got to be more to it than tuning; there must be some amazingly bad software architecture -- from a novice's point of view, a 4 MB Macintosh runs a far more efficient, interesting system than a 16 MB Indy. The Mark Segal quote above sums it up.

Code walk-throughs and design reviews are in order for most of our software. The attendees should include not only people working in the same area, but a small cross-section of experienced engineers from other areas. Get a pool of, say, 20 experienced engineers and perhaps 3 at a time would sit in on code reviews together with the other people working in that area.

Code reviews will help in many ways -- the engineer presenting the code will have to understand it thoroughly to present it, others will learn about it, and outside observers will provide different ways to look at the problems.

The most important thing should be the focus -- we're trying to make the code better and faster, not to make it more general, or have new features, or be more reusable, or better structured.

For complex problems, the walk-through should also include some general design review. Are these daemons really necessary? Do we really need this feature? And so on.

Fixing Bugs:

The code walk-throughs will obviously tend to turn up some bugs, so they'll serve a dual purpose.

With 500 or so priority 1 and 2 bugs, we must prioritize these as well. A bug that causes a system crash only on machines with some rare hardware configuration is properly classified priority 1, but it's probably less important than a bug in a popular program like Showcase that causes you to lose your file every tenth time, which would normally rank as priority 2. The effort involved in the fix should also be taken into account. For bugs of equal frequency of occurrence, it's probably better to fix 20 priority 2 bugs than 1 priority 1 bug if the priority 2 bugs are 20 times easier to fix.

A bunch of bugs can be eliminated by getting rid of features. Let's have the courage to cut some of the fat.

WHAT TO DO -- LONG TERM

"Software quality is not a crime."

-- Unknown (seen on a poster in building 7)

It's easy to go on forever here, but I'll try to limit it to a few key ideas. We don't have to do all these at once, but we'd better start.

Have an overall SGI software plan.

Let's get an architect, or at least a small group of highly technical people, not just managers, to agree on plans for releases. In fact, since the release is a company-wide project, there ought to be company-wide participation in the decisions of what's in a release. The group should include marketing, documentation, engineering, and management and should come up with a compromise that's reasonable to all.

In every case, some attempt must be made to check reasonableness all the way to the bottom. There's a long series of excuses, "Well, that's what my junior VPs told me.", or "That's what my directors/managers/lead engineers/engineers told me." We get killed by the optimist effect, and a disinclination to listen seriously to anyone but our direct reports. Try to imagine the guts it takes for an engineer to go to his director and say: "My manager's out of his mind -- I can't possibly do what he's promised."

Let's try to concentrate on performance and quality, not on new features, especially for the 5.1.2 release. I know from my own experience that when I write good code, I spend 10% of the time adding features, and 90% debugging and tuning them. It's the only way to make quality software. In SGI's recent releases, the opposite proportions are often the rule. It's much easier to add

100 really neat features that don't work than to speed up performance by 1%.

Aim for simplicity in design, not complexity. Make a few things work really well; don't have 1000 flaky programs.

Be willing to cut features; who's going to be more pissed off: a customer who was promised a feature that doesn't appear, or the same customer who gets the promised feature, and after months of struggling with it, discovers he can't make it work?

Get better agreement between the top level VPs and the lowest engineers that a given schedule is reasonable.

For new development, continue the formal design reviews and code walk-throughs. These shouldn't just happen once in the development cycle -- things are bound to change, and code reviews can be very valuable, even for our experienced programmers.

ACKNOWLEDGEMENTS

I take full responsibility for the opinions contained herein, but I'd like to thank Mark Segal, Rosemary Chang, Mary Ann Gallager, Jackie Neider, Sharon Fischler, Henry Moreton, and Jon Livesey for suggestions and comments.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Search RISKS using swish-e

THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 15: Issue 81

Friday 29 April 1994

Contents

Boot Prom commits Denial of Service Attack

Dave Wortman

Cyrix 486 CPU Bug

Dave Methvin

Call Identifier (tm) forgets list of received calls

Robert Chesler

Re: Unwanted FAX received via voicemail

Declan A. Rieb

Re: Stress Analysis of a Software Project

Tom Davis via Joan Eslinger

A. Padgett Peterson

Inspecting Critical Software

David Parnas via Jan Arsenault

Info on RISKS (comp.risks)

✓ Boot Prom commits Denial of Service Attack

Dave Wortman <dw@pdp1.sys.toronto.edu> Fri, 29 Apr 1994 12:52:08 -0400

A major power outage here on Tuesday demonstrated the risks of excessive automation and administrative convenience.

Our computing environment consists of a heterogeneous network of Sun, Dec and IBM workstations and related fileservers.

When a Sun workstation boots up, a hardware prom issues a rarp request to establish the workstations network address and to identify a server that can provide it with a bootprogram and then the Unix kernel.

The boot prom uses the trivial file transfer protocol (tftp) to request the boot program. It initially issues a tftp request to the server it has identified, but if that tftp request times out then it broadcasts a tftp request on its local network looking for any server that can provide it with a bootprogram. It keeps repeating this process until it receives a boot program.

One the Suns the prom has no builtin knowledge of its network address or the network address of the server.

There are some good reasons for keeping the boot prom ignorant of its network environment and using a broadcast protocol, including the administrative convenience of not having to do anything to workstations when the server changes and providing a degree of robustness in a multi-server environment.

In recent years there have been security problems related to the tftp protocol so in our environment the Dec workstations run security monitoring software that keeps a log of failed tftp attempts to help detect potential intruders. The security software writes a log file of failed tftp requests and also puts a message on the affected machines console.

What got us into trouble after the power outage was that the Sun workstations came back online but the corresponding Sun servers came up in a wedged state in which they responded to the initial rarp request but then failed to respond to any workstations tftp request for a boot program.

After the initial tftp request to the Sun server timed out, our network was flooded with tftp requests from many Sun workstations all trying to find any server that could boot them.

In the meantime the Dec workstations on the network had rebooted successfully and were being used by a number of professors and students. However, these machines soon became unusable due to the effort required to deal with the flood of tftp requests. The security monitoring software contributed to this problem by writing messages to each machines console window (ignorable but consumptive of resources) and by almost filling up a critical file system with its log files. If this filesystem had filled up, the machines would have been totally unusable. Even if we hadn't been running the security monitoring software, usability of these workstations would have been impaired by the handling of the tftp requests.

There are several things that could have been done better:

- the question of whether falling back to a broadcast protocol for booting is the right approach should be reexamined. On most systems the set of servers that could successfully respond to a boot request is a) small, b) well-known, and c) changes very slowly over time.
- the boot proms should use some form of backoff strategy when the tftp requests consistently fail to avoid overloading the network.
- our security logging software needs to be more robust in dealing with its log files. Waiting until a log file write fails due to a full filesystem is too late if the full file system will cause other processes to crash. This is tricky since we don't want a introduce a mechanism that would allow an intruder to overwhelm the security software with failed attempts and then proceed to do dirty work once logging has been suspended due to log file overflow.

A curious legal question comes to mind: could the manufacturer or the proprietor of the workstation containing boot prom be held

guilty of a "denial of service attack" on our Dec workstations? If an individual had issued all of those tftp requests we certainly would be considering the question.

✓ Cyrix 486 CPU Bug

Dave Methvin <0003122224@mcimail.com> Fri, 29 Apr 94 07:40 EST

I'm an editor at Windows Magazine. In our May issue I wrote a news story reporting a bug in the Cyrix Cx486DX CPU. The Cyrix Cx486DX was designed to be completely software-compatible with Intel's i486DX processor. However, Ed Curry of Lone Star Evaluation Labs (LSEL) found a bug relating to floating-point operations while doing some in-depth compatibility testing. Cyrix shipped thousands of chips with this bug before April 1994, but has now fixed the problem.

The bug occurs when a register load instruction (such as MOV reg,mem) is followed by an instruction that clears the floating-point status register (FCLEX). If the memory location being referenced is in the CPU's internal cache, the MOV instruction works fine. If, however, the MOV requires an external bus cycle, executing the FCLEX instruction aborts the cycle. As a result, the register is not loaded properly.

The risk here is that someone may run software on the Cx486DX that generates incorrect results where an i486DX would work fine. The Cyrix position is that this is a minor bug and that we (Windows Magazine and LSEL) are making too much of it. However, LSEL has seen the bug in their test code compiled under OS/2 and Windows NT. The test code performs typical engineering and scientific calculations, so it's not contrived or artificial. We have not found the problem in any shrink-wrapped application. Most MS-DOS and Microsoft Windows insert a FWAIT instruction before any floating-point instruction, so they generally won't exhibit the problem.

What does the Risks readership think? Are we making too much of this? Is anyone out there using PC with a Cx486DX?

Call Identifier (tm) forgets list of received calls

Robert Chesler <rob@chesler.absol.com> Fri, 29 Apr 94 13:28:10 -0400

I accepted a no-installation-cost trial of Caller ID and found it somewhat useful for correlating call times with answering machine messages, but found 90% of my received calls were out of my area and thus had no number actually displayed, only the date and time.

Last night I noticed that the box had cleared out its memory.

No call had been received on that line between the time I had last checked it and the time I noticed it with an empty list.

The risk here is that if some message was sent to the box through the phone line to clear its list, then the box would be less useful for someone using the box to catch a crank caller or even log when important calls or messages were received. If the caller ID protocol includes such a message, then such a message could undoubtedly be faked if someone got physical access to a residence's network interface or telephone company signalling.

I'm sure that boxes more advanced than the promotional box that was given to me might have precautions or a printed log, but I would imagine that the promotional boxes are widely used.

--Robert

Unwanted FAX received via voicemail

"Declan A. Rieb" <darieb@sandia.gov> Tue, 26 Apr 1994 15:09:57 -0600 (MDT)

The voicemail system I use allows incoming FAXs to be saved and handled as messages. Upon receipt, the system notifies the user that there is an incoming fax message, and you can even query for the number of pages. When a message exists in the "voice mailbox", one can have the system forward it to a real FAX machine (either a preselected "primary" FAX or any other phone number.) Requesting such a forward places the FAX message into a queue, meaning it may actually be sent at some future time.

Last week I received a 5-page FAX message. It did not come from a local caller (one on the same telephone switch.) All I knew was that it was five pages. I sent it off to my primary printer, and an hour or so later went to pick it up. No FAX for me there. I tried again. No FAX for me. FAX machine broken? After a day of this, I sent the FAX to a machine and promptly went to watch. Out came a list of imported tequila prices, and several blank pages! I recalled seeing several such lists at the other FAX machines...But none were addressed to me! Surely they weren't mine...but a closer inspection showed that the FAX phone number listed was indeed mine (perhaps a missing area code?)

Whoa! that kind of business is illegal here! And I've been spreading the things around the area. At least I didn't have my name on them, but the phone number was mine!

Welcome to the wonderful world of hi-tech. It used to be that FAX machines were relatively rare, and "dialing" a wrong number would mean the FAX doesn't get sent. Now, EVERY phone here can receive a FAX, and we can send multiple copies out without knowing what it is we sent! Yes, I'll be a bit more careful in the future.

[A surprising number of readers chided me for NOT having appended a "You mean a FAX PAS? PGN" appendum. THANKS! PGN]

Re: Stress Analysis of a Software Project (Davis/Leichter R-15.80)

Joan Eslinger <wombat@kilimanjaro.engr.sgi.com> Fri, 29 Apr 1994 19:35:15 GMT

The memo Jerry Leichter posted was an actual Silicon Graphics memo. However, life for Silicon Graphics and Tom Davis is not quite so bleak as some might think. Tom Davis wrote the original memo to point out problems and ask everyone to help fix them.

It was very effective. I installed a beta version of the new 5.2 release on my Indy in January, and only rebooted the machine a couple of weeks ago because I was moving to another building. Sure, I had to add another swap file on-the-fly about once a month because my emacs processes grew so large :-), but the system did not crash. And performance is quite snappy. "Watch the skies."

Since the memo has been popping up all over the net, Tom has written a reply to it, included below. There isn't really a RISKS tie-in, unless you count the risk of having only the "bad" half of a story get wide distribution.

Joan Eslinger / Silicon Graphics / wombat@sgi.com

I am the author of the original memo below, which was intended for internal Silicon Graphics use only, and was not for anyone outside the company. But since it has been leaked to the net, and is beginning to be used by competitor's sales people, I feel a response is required.

I don't believe that these problems are unique to Silicon Graphics. >From discussions with friends who are insiders in many different companies, I am certain that similar memos could be written about the software of each of our competitors.

What I like about working for Silicon Graphics is that at least here, something is being done about it -- I worked for companies in the past where the response would have been to stick our heads in the sand in hopes that the problems would just fix themselves. If I hadn't thought that the memo would catalyze some change here, I wouldn't have written it.

The details appear as comments to my original article below. Luckily, the article is 6 months old, and we have had a chance to make some significant progress.

Typically, what happens is that each faster generation of hardware is followed by software that more than compensates for the increased speed, but as a result of this memo, Silicon Graphics has been able to skip one of the slowing software cycles, making, instead, a performance and quality based release. The next release is going to be similar, and in the meantime, we get an extra hardware boost from the faster

R4600 processors.

-- Tom Davis Silicon Graphics

General comments:

As a fairly direct result of this memo, SGI decided not to continue "business as usual" in software development. The approach we took to the problem was the following:

With the 4.0.5abcdefghi... fiasco, and the fact that the 5.* releases were still for specific machines, our developers were desperate for an all-platforms release. We decided to make such a release relatively soon -- and 5.2 actually MRed in February. The 5.2 release had two goals -- primarily, all-platform, and given that it went out in February, do as much performance-tuning and bug-fixing as time allowed.

In that period, the performance on 16MB systems was essentially doubled, which improved performance on larger systems as well, but to a lesser degree. Significant numbers of bugs were fixed as well.

Some people hoped that a few quick fixes would bring back all the performance in 5.2, but a little investigation indicated that was a list of things to be done, and that another quality release would be required.

The 5.3 release, not officially scheduled, but which should be MRed around October or November is that quality (performance and bug-fix) release. We'll add a few new features, but they will be the exception rather than the rule. The longer time before the 5.3 release should give us time to do a thorough job of solving our problems.

For 5.3, there's also time to set up solid performance and bug-fixing goals, and these are already being discussed.

And most important -- the worst problems were with 16 MB systems that paged their brains out. They are better now, but not great. But we don't sell them. One of the 5.3 goals is to improve performance (or reduce sizes enough) that it will be acceptable on a 16 MB machine.

The kernel memory leaks are all fixed, and many of the important programs have been reduced in size. For 5.2, 5 or 6 of our most heavily-used programs were subjected to close scrutiny to find out where the performance went, and many were significantly improved.

A lot more work is planned for 5.3 to reduce the sizes of the executables.

Work is continuing on the DSOs to split them up properly so that they don't all have to be loaded, and to improve their performance and start-up time. We're working to make "quick-starting" happen more automatically.

> PERFORMANCE UPDATE

I don't think it's unusual to do benchmarks with non-standard compiler settings. Both we and our competition have done so for a long time. We do ship all the libraries, et cetera, necessary to duplicate these results so customers for whom speed is the only objective can pay the cost of larger executables in exchange for the added speed.

Unfortunately, I can't re-run some of these tests, but 5.2 is definitely better than 5.1.

I think the 5.1 fiasco has caused a lot of our management to see the light, and in conversations with people at all levels, it's clear that nobody wants to see anything like it happen again. The 5.2 and future 5.3 releases seem to be steps in the right direction.

But there's still a lot of work to do, and we in engineering can use every minute between now and the 5.3 release to improve things.

The 5.3 release is being planned with reasonable beta-cycles, and with enough time between now and "code freeze" to make significant improvements.

> Management Issues:

I think this sort of disconnect is not too unusual -- there is always enormous pressure to announce a very low entry price-point, and the 16MB system provided that. Everybody does this with the full knowledge that on a minimum system, you won't be able to run many interesting applications, and almost everyone will have to purchase a bit more memory. It's just that in the case of Indy, there were so many new features that the proposed minimal system was embarrassingly slow.

The "fix" is simply not to ship the 16MB systems which will insure that everyone will get a very usable machine. All we really lose is our low entry price point, and the gain is that we won't have to deal with the few irate customers who bought a minimal system.

Although some of our performance loss is due to more complicated features, the vast majority is due to the fact that more memory is required, and without it, the systems page with a consequent dramatic reduction in performance. The 4.0.X -> 5.X change on our large machines was measurable, but not nearly so noticeable as on the smaller ones.

We're still not completely there (as far as I can tell) with respect to better software management. The good thing is that many of our higher-level managers are acutely aware of the problem now -- Forest Baskett and Tom Jermoluk are extremely concerned, for example.

It's too bad it took a shock like 5.1 to make everybody take notice, but

at least they did, and we're doing the right sorts of things to correct it.

[Moderator deleted the entire interstiated message from RISKS-15.80. PGN]

★ Re: Stress Analysis of a Software Project (Davis/Leichter R-15.80)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com> Fri, 29 Apr 94 08:22:09 -0400

For years, people have been postulating projects that are too complicated to comprehend and we have seen several examples of what happens when this occurs. IMHO the only solution is to separate functions into stand-alones that utilize a common and understandable foundation and which are understandable.

Where many have felt that a single integrated system is best, I have often been called in to "put out fires" and the first thing I do is to separate the problem into "atoms", the least divisible pieces. It is astounding how often problems that cannot be seen when tightly wrapped in a package becomes obvious when viewed by itself. Sometimes you just can't see the tree for the forest.

- > Some people claim that we need new software debugging tools to look at
- > the problem, and that may be true, but it's not a short-term solution,
- > and it runs the risk of causing us to spend all our time designing
- > performance measurement tools, rather than fixing performance.

This is disturbing. Unless you have the tools to properly examine a system you cannot tell what is really going on and the reccuring theme of the memo seems to be that no-one knows. Without the proper tools, the job will never be completed.

Again I can only speak from personal experience but cannot count the times when called in to fix a problem that supervisors have gotten very antsy waiting for something to happen while the envelope is being defined. Have found that unless the system is understood, it *can't* be fixed (see "little silver hammer" syndrome).

The problem with the engineers also appears symptomatic. Engineers are supremely good at taking a concept and making it work. They are not generally good at determining that a concept is flawed in the first place, instead often they will continue to work as if the concept were correct and they were just lacking in skill. This leads to precisely the morale problems described.

The major problem with engineers is that they accomplish the impossible so often that the marketeers come to expect it from them.

The real problem seems to be simply "no-one in charge" and is all too common in large organizations. History is rife with examples of companies, states, countries that became too concentrated at the top and fell victim to the huns/vandals/Standard Oil as they rose to power. "Think of it as Evolution in Action" - Jerry Pournelle

Padgett

Inspecting Critical Software, a course by David Parnas

<arsenau@mcmail.cis.mcmaster.ca> Tue, 26 Apr 94 20:43:34 EDT

Inspecting Critical Software: An Intensive 3-day Course offered by The Faculty of Engineering, McMaster University, Hamilton, Ontario, Canada

Taught by Prof. David Lorge Parnas, with the support of TRIO

June 7, 8, 9, 1994

1. Background

Software is critical to the operation of modern companies and is frequently a key component of modern products. Some pieces of software are particularly critical; if they are not correct, the system will have serious failures. Standard methods of software inspection are not systematic. This course teaches a procedure for software inspection that is based on a sound mathematical model and can be carried out systematically by large groups.

The software inspection procedure combines methods used at IBM, work originally done at the U.S. Naval Reserve Laboratory for the A-7E aircraft, and procedures applied to the inspection of software at the Darlington Nuclear Power Generating Station. The method has been refined and enhanced by the Software Engineering Research Group at McMaster University's Communication Research Laboratory. It can be applied to software written in any imperative programming language.

2. What Will Participants Learn?

Participants in the course should return to their workplace with an understanding of the way that mathematics can be used to document and analyze programs. They will also return with documentation of a piece of their employer's code that can be used to explain the work to others.

3. Programme

Day 1 Predicate Logic and Program-Functions/Relations

- Overview and Case Study
 A discussion of previous applications of the method.
- Predicate Logic
 The inspection method is based on predicate logic, which will be reviewed in this section.
- 3) Tabular Expressions
 This session will be devoted to the writing of readable
 predicates using two-dimensional notations rather than classical
 one-dimensional expressions. There will be numerous examples.
 Participants will be taught to read and write tabular expressions.
- 4) Describing Program Function

This session will be devoted to writing program descriptions using predicates and tables.

Day 2 Inspection of Dijkstra's Dutch National Flag Program

Participants will be given a copy of E.W. Dijkstra's explanation of a program along with several sample programs. They will be asked to apply the inspection method and approve or reject each program. The instructor and some assistants will be available as consultants during this process.

Day 3 Morning: Inspection of a "Real" Program

Working in small groups, the participants will take a section of a program from their company and inspect it using the method learned so far, producing documentation as they go. Day 3 Afternoon: Report on the Inspection Results, Discussion of Testing

The first part of the afternoon will be devoted to a series of reports by the participants on the results of their efforts in the morning. The remainder of the afternoon will be devoted to a discussion of the interaction between testing and inspection. We treat testing, not as an alternative to inspection, but as complementary to inspection. We discuss the way that the documentation produced in the inspection process can be used in the testing process.

4. Learning By Doing

The course is language-independent. In fact, on the third day, participants will inspect code written in any language that they use in the workplace. This course presents an approach to active design reviews that has the reviewers writing precise documentation about the program and explaining their documentation to an audience of other reviewers. A significant part of each day will be spent using the ideas that have been presented to determine whether or not programs do what they are supposed to do. On the last day, participants will inspect a small program that they brought with them from their company. Participants should leave the course with improved ability to inspect software.

5. Who Should Attend?

Participants should be experienced programmers and not afraid of learning a little mathematics. The mathematical basis for the method is classical and takes up only a few hours in the course. However, it is fundamental to understanding the method. It is expected that the participants will be used to reading code written by others and it will be helpful if they can read Pascal.

6. What Should You Bring With You?

For the exercise on the third day, each participant should bring a small program, perhaps 50 lines that are critical to some project. It need not be "mature" code, but it should compile and have survived some testing or use. If there are several participants from the same company, they may work in small groups on slightly larger programs. You may want to bring a reference manual and some conventional documentation about the

program with you. It will help if one of the participants is familiar with the program.

7. The Instructor

The course will be taught by Prof. David L. Parnas, an internationally recognized expert on Software Engineering. Dr. Parnas initiated and led the U.S. Navy's Software Cost Reduction Project, where the tabular notation was first used, advised the AECB on the use of these methods at Darlington, worked with IBM's Federal Systems Division, leads the Software Engineering Research Group at McMaster University and is a Project Leader for the Telecommunications Research Institute of Ontario.

Information about costs, registration, etc. can be obtained from: Jan Arsenault, Faculty of Engineering, JHE-201A, McMaster University, 1280 Main Street West, Hamilton, ON, Canada, L8S 4L7.

Telephone: 905 525 9140 x 24910 email: arsenau@mcmail.cis.mcmaster.ca



Search RISKS using swish-e

Report problems with the web pages to the maintainer